

# Information regarding

## LANCOM GS-23xx(P/+)

Copyright (c) 2002-2014 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.eu>  
02.08.2016, CBuersch

### Table of Contents

<b>1. Preface.....</b>	<b>2</b>
Warning hints .....	2
Hint for firmware update from <= 1.48 RC1 to >= 1.65 Rel .....	2
Hint for firmware update to 3.17 Rel .....	2
<b>2. Known Issues .....</b>	<b>2</b>
<b>3. New Features, Improvements and History .....</b>	<b>3</b>
LANCOM GS-23xx(P/+) improvements 3.17 Rel ▶ 3.22.0003 Rel.....	3
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 3.10 Rel ▶ 3.17 Rel .....	3
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 2.83 Rel ▶ 3.10 Rel .....	4
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 2.52 Rel ▶ 2.83 Rel .....	5
LANCOM GS-2326(P) / GS-2352(P) improvements 2.26 Rel ▶ 2.52 Rel .....	6
LANCOM GS-2326(P) / GS-2352 improvements 1.65.Rel ▶ 2.26 Rel.....	7
LANCOM GS-2326 / GS-2352 improvements 1.48 RC1 ▶ 1.65 Rel.....	7
LANCOM GS-2326 / GS-2352 improvements 1.32 Rel ▶ 1.48 RC1 .....	7
<b>4. Comments .....</b>	<b>8</b>

## 1. Preface

### Warning hints

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

### Hint for firmware update from <= 1.48 RC1 to >= 1.65 Rel

Before updating from any firmware older than 1.48 RC1 to firmware 1.65 Rel or newer you have to install firmware 1.54.

A direct update to 1.65 Rel is **not** possible.

A downgrade to any firmware prior 1.54 is not possible afterwards.

### Hint for firmware update to 3.17 Rel

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.

### Procedures

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

Switches running firmware version 2.xx - 2.83 can be directly updated to firmware version 3.17.

Switches running firmware version 3.10 have to be powered off once. This is mandatory.

2. LANCOM GS-2352P:

Switches running firmware version 2.xx - 2.83 can be directly updated to firmware version 3.17.

Switches running firmware version 3.10 have to be powered off once. This is mandatory.

If you get an out of memory message when updating a LANCOM GS-2352P to firmware 3.17, you have to install firmware 3.04a first.

Afterwards you can proceed with the update to firmware 3.17.

## 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

#### LANCOM GS-23xx(P/+) 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 deleted 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 switch'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 selected 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.