

LANCOM Release Notes für GS-23xx



3.32 RU7

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

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

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

23.10.2020, MKoser

Inhaltsübersicht

1. Einleitung	2
2. Vorgehensweisen zum Firmware-Update	2
Hinweis zum Software-Update auf LCOS SX 3.32	2
3. Neue Features, Änderungen und Historie	3
LANCOM GS-23xx Änderungen 3.32.0222 RU7	3
LANCOM GS-23xx Änderungen 3.32.0221 SU6	4
LANCOM GS-23xx Änderungen 3.32.0210 RU5	4
LANCOM GS-23xx Änderungen 3.32.0208 RU4	4
LANCOM GS-23xx Änderungen 3.32.0135 SU3	5
LANCOM GS-23xx Änderungen 3.32.0114 RU2	6
LANCOM GS-23xx Änderungen 3.32.0110 RU1	6
LANCOM GS-23xx Änderungen 3.32.0012 Rel	7
LANCOM GS-23xx Änderungen 3.30.0450 RU4	8
LANCOM GS-23xx Änderungen 3.30.0417 RU3	9
LANCOM GS-23xx Änderungen 3.30.0324 RU2	9
LANCOM GS-23xx Änderungen 3.30.0321 RU1	9
LANCOM GS-23xx Änderungen 3.30.0204 Rel	10
LANCOM GS-23xx Änderungen 3.30.0115 RC1	10
LANCOM GS-23xx Änderungen 3.22.0003 Rel	11
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 3.17 Rel	11
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 3.10 Rel	12
LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 2.83 Rel	13

Inhaltsübersicht - Fortsetzung

LANCOM GS-2326(P) / GS-2352(P) Änderungen 2.52 Rel	14
LANCOM GS-2326(P) / GS-2352 Änderungen 2.26 Rel	15
LANCOM GS-2326 / GS-2352 Änderungen 1.65 Rel	15
LANCOM GS-2326 / GS-2352 Änderungen 1.48 RC1	16
4. Allgemeine Hinweise	17
Haftungsausschluss	17
Support-Hinweise & bekannte Einschränkungen	17

1. Einleitung

LCOS SX ist das Betriebssystem für alle LANCOM Switches. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS SX-Version für alle LANCOM Switches verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS SX Software Release 3.32 RU7 sowie die Änderungen und Verbesserungen zur Vorversion.

Bitte **sichern Sie** vor dem Update Ihrer LANCOM-Geräte auf eine neue Firmware-Version **unbedingt Ihre Konfigurationsdateien!**

Aufgrund der teils umfangreichen Feature-Erweiterungen ist ohne eine solche Sicherung ein **Downgrade** auf die alte Firmware **nicht mehr automatisch möglich**.

Bitte beachten Sie, dass für Ihr Gerät unterschiedliche Firmware-Dateien zur Verfügung stehen können.

2. Vorgehensweisen zum Firmware-Update

Hinweis zum Software-Update auf LCOS SX 3.32

Bei einem Firmware-Update von der Version 2.83 oder älter wird der Flash-Speicher des Gerätes einmalig neu programmiert. Hierdurch verlängert sich die Dauer des Updates je nach Gerät auf bis zu 15 Minuten.

Trennen Sie den Switch während des Firmware-Updates niemals vom Stromnetz, da das Gerät bei einem Abbruch des Aktualisierungsvorganges nicht mehr ordnungsgemäß startet.

Für LANCOM Switches der Typen GS-2326(+)/GS-2326P, GS-2352 und GS-2310P

Wenn der Switch mit einem LCOS SX der Versionen 2.83 oder älter betrieben wird, so ist vor dem Update auf Version 3.32 ein Zwischenupdate auf die Version 3.17 erforderlich.

Für LANCOM GS-2352P

Wenn der Switch mit einem LCOS SX der Versionen 2.83 oder älter betrieben wird, so ist vor dem Update auf Version 3.32 ein Zwischenupdate auf die Version 3.04a erforderlich.

3. Neue Features, Änderungen und Historie

Geräte, die mit LCOS SX 3.30 oder größer ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme von neuen Geräten. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität jederzeit auf der WEBconfig-Oberfläche unter Konfiguration > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

LANCOM GS-23xx Änderungen 3.32.0222 RU7

Korrekturen / Anpassungen

- > Bei einer MAC-based 802.1X-Authentifizierung gegen einen RADIUS-Server wurde ein Client authentifiziert, obwohl die RADIUS-Authentifizierung mit einem ‚RADIUS Reject‘ und ‚EAP Success‘ beantwortet wurde. Das EAP-Paket vom Typ ‚Success‘ bezieht sich jedoch nur auf die erfolgreiche EAP-Kommunikation. Der Switch interpretierte nur den EAP-Teil, aber nicht den Inhalt des RADIUS-Pakets (das ‚RADIUS Reject‘). Deshalb wurde ein Client, welcher nicht auf dem RADIUS-Server bekannt war, ebenfalls erfolgreich authentifiziert.
- > Der Switch ist jetzt in der Lage, die RADIUS-Attribute ‚NAS Identifier‘ und ‚Service Type=Call Check‘ zu übermitteln.
- > Die maximale Länge eines SSH-Hostkey wurde von 1024 Bit auf 2048 Bit erweitert.
- > Eine MAC-based 802.1X-Authentifizierung gegen einen RADIUS-Server wurde als RADIUS-Request ohne EAP-Bestandteile und mit der MAC-Adresse als Benutzername übergeben.
- > Bei Verwendung einer 802.1X-Authentifizierung mit den Modi ‚Single 802.1X,‘ ‚Multi 802.1X‘ und ‚MAC-based Auth.‘ wurden nach dem erfolgreichem Login der Endgeräte die MAC-Adressen nicht in die MAC-Adress-Tabelle übernommen.

LANCOM GS-23xx Änderungen 3.32.0221 SU6

Korrekturen / Anpassungen

- › Spezielle Benutzereingaben über das Webinterface wurden nicht korrekt validiert. Dadurch konnte ein unvermittelter Neustart des Gerätes provoziert werden.

LANCOM GS-23xx Änderungen 3.32.0210 RU5

Korrekturen / Anpassungen

- › Beim Betrieb von LANCOM Switches der GS-23xx-Serie konnte es vorkommen, dass Geräte nach einem Neustart ihre Seriennummer und MAC-Adresse verloren und auch keine IP-Adresse mehr beziehen konnten. Der Betrieb der Geräte war weiterhin gegeben, die betroffenen Switches konnten jedoch nicht mehr über ihre IP-Adresse erreicht werden.

LANCOM GS-23xx Änderungen 3.32.0208 RU4

Neue Features

- › In der ‚Authentication Method Configuration‘ besteht nun die Möglichkeit, die Protokolle HTTP und HTTPS getrennt zu konfigurieren.
- › Vereinfachung der VLAN-Portmarkierung
- › In der ‚System Log Configuration‘ wird nun eine Warnung bei unsicherer ‚SNMPv2 Get community‘-Konfiguration angezeigt.

Korrekturen / Anpassungen

- › Die in den Konfigurationsdateien hinterlegten Passwörter werden nun verschlüsselt abgespeichert.
- › Bei Verwendung von 802.1X mit dem Authentifizierungs-Modus ‚Mac-based Auth.‘ konnte die Funktion ‚RADIUS-Assigned VLAN Enabled‘ nicht aktiviert werden.
Es wurde ein neuer Authentifizierungs-Modus ‚MAC-based single Auth.‘ implementiert, mit dem die Verwendung der Funktion ‚RADIUS-Assigned VLAN Enabled‘ möglich ist.
- › Obwohl der Zugriff auf das Webinterface in der Konfiguration gesperrt war, wurde bei einem Zugriffsversuch die Login-Seite des Webinterfaces angezeigt. Ein Login war jedoch nicht möglich.
- › Nach Deaktivierung von ‚Web‘ in der ‚Authentication Method Configuration‘ wurde der Port 80 als offen angezeigt, ein Zugriff auf die Web-Oberfläche war jedoch nicht möglich.
- › Bei Verwendung des Features ‚Port Based 802.1X‘ und dem VLAN-Modus ‚Trunk‘ konnte ein angeschlossenes Gerät zwar authentifiziert werden, eine Datenübertragung war aber nicht möglich.

- In der SNMP-MIB eines LANCOM GS-2310(P)(+) wurden bei aktivem LACP im Baum LLDP 13 Ports ausgegeben, obwohl der Switch nur über 12 Ports verfügt.
- Wurde auf dem Switch ein Voice VLAN konfiguriert, war sporadisch die MAC-Adresse von einzelnen angeschlossenen Netzwerk-Geräten nach dem Ablauf der ‚Voice VLAN Aging Time‘ nicht mehr in der MAC-Address-Tabelle enthalten. Dadurch konnten diese Geräte nicht mehr im Netzwerk kommunizieren. Es waren nur Geräte in VLANs betroffen, die nicht dem Voice VLAN entsprachen.
- Beim Setzen eines statischen MAC-Tabellen-Eintrags im Menü ‚Filtering Data Base / Configuration‘ startete der Switch unvermittelt neu
- Wurde ein Port-basiertes VLAN konfiguriert und zusätzlich eine Konfiguration für MAC-basiertes VLAN hinzugefügt, funktionierten nur noch die MAC-basierten Einstellungen; die weitergehenden Einstellungen wurden ignoriert.
- Das (Admin)-Passwort, der User-Name und der Privilege Level ließen sich nicht per SNMP mit dem bereits vorhandenen Admin-Account konfigurieren.
- Die Funktion ‚Limit Control‘ im Menü ‚Security / Port Security‘ konnte nur über die Web-Oberfläche aktiviert werden. Wurde versucht, die Funktion über die Konsole zu aktivieren, wurde die Fehlermeldung „Port Security Limit Control Configuration of easyport must be preserved“ ausgegeben.
- Auf der Konsole gab es keine Möglichkeit, mehrere Protokolle für den Zugriff auf den Switch gleichzeitig zu aktivieren (z.B. SNMP & TELNET/SSH). Es konnten entweder alle Protokolle gleichzeitig oder nur ein Protokoll aktiviert werden.

LANCOM GS-23xx Änderungen 3.32.0135 SU3

Korrekturen / Anpassungen

- Der Zufallsgenerator zur Erzeugung von SSH-Schlüsseln generierte nicht genügend unterschiedliche Host-Schlüssel. Um sicher zu stellen, dass nach der Firmware-Aktualisierung auf LCOS SX 3.32 SU3 genügend unterschiedliche SSH-Host-Schlüssel im Switch zur Verfügung stehen, müssen Sie folgendermaßen vorgehen:
 - Öffnen Sie das Webinterface des Switches.
 - Wechseln Sie in das Menü ‚Security / SSH‘.
 - Klicken Sie dort auf die Schaltfläche ‚Regenerate Hostkey‘.
 - Speichern Sie die Konfiguration im Menü ‚Maintenance / Save/Restore‘ mit der Option ‚Save Start‘.
 - Starten Sie den Switch mit der Option ‚Maintenance / Restart Device‘ neu.
 Beim Neustart des Switches werden neue SSH-Host-Schlüssel erzeugt.
 Siehe auch <https://support.lancom-systems.com/knowledge/x/AoCCAg>.

LANCOM GS-23xx Änderungen 3.32.0114 RU2

Korrekturen / Anpassungen

- Bei Switches, welche mit der LANCOM Management Cloud (LMC) verbunden waren, konnte es in seltenen Fällen zu einem SSL-Verbindungsfehler kommen, der dazu führte, dass die Geräte nicht mehr von der LMC verwaltet werden konnten. Lediglich das Monitoring war noch funktional.
- Wenn der LANCOM Switch einen Netzwerk-Loop erkannt hatte, wurde bisher lediglich die Uhrzeit und der blockierte Port in einer Syslog-Meldung protokolliert. Die Netzwerk-Loop-Erkennung protokolliert nun zusätzlich die Nummer des zweiten beteiligten Ports und gibt zudem eine Information darüber, welcher Port der Sender und welcher Port der Empfänger des Loop Protection Frame war.

LANCOM GS-23xx Änderungen 3.32.0110 RU1

Neue Features

- Erweiterung der Gerätelogs
- Erweiterung der PoE-Detection (Legacy Mode)
- Neuer Schalter für sFlow (Always On)

Korrekturen / Anpassungen

- Wurde einem per LMC verwalteten Switch per Addin-Skript eine feste IP-Adresse zugewiesen, führte dies zu einem unvermittelten Neustart des Switches.
- Die LANCOM Switches übermittelten MAC-Adressen (z. B. von Supplicants bei 802.1X an einem RADIUS-Server) ausschließlich unter Verwendung von kleinen Buchstaben (z. B. 00-10-a4-23-19-c0). Laut der RFC-3580 müssen jedoch Großbuchstaben verwendet werden (z.B. 00-10-A4-23-19-C0), was nun der Fall ist.
- Erstellte man eine Skriptspeicherung von einem Switch des Typs **LANCOM GS-2352x**, in welcher bei 26 Ports ein PVID eingetragen ist, so ließ sich diese Skriptspeicherung nicht in das Gerät laden.
- Wenn auf einem in der LMC verwalteten LANCOM Switch der GS-23xx-Serie die LLDP-Funktion für die automatische Geräte-Erkennung verwendet wurde, konnte es zu einem unvermittelten Neustart des Switches kommen.
- Die automatische Umstellung der Uhrzeit auf mitteleuropäische Sommerzeit (MESZ) erfolgte eine Woche zu früh.
- Ein Ping auf die IP-Adresse eines GS-2352(P) wurde vom Switch nicht beantwortet, wenn ein Management-VLAN ungleich 1 verwendet wurde.
- Bei der Übernahme eines GS-23xx in die LANCOM Management Cloud wurden „Forbidden VLANs“ nicht in die LMC-Konfiguration übernommen.
- Debug-Informationen zur Analyse eines unvermittelten Neustarts („Watchdog“) konnten per SSH und Telnet nicht vollständig ausgelesen werden.
- Eine offene SSH-, Telnet- oder Web-Session auf einen über die LMC verwalteten Switch wurde nicht unmittelbar beendet, wenn über die LMC ein neues Hauptgerätepasswort auf den Switch ausgerollt wurde.
- Ein Reboot-Event, welches über SNMP oder die LMC ausgelöst wurde, wurde nicht ins Syslog geschrieben.

- Das Pairing eines Switch mit der LMC über **LANconfig mittels Aktivierungscode** wurde nicht erfolgreich abgeschlossen. In der Folge befand sich der Switch in einer Endlos-Schleife. Der identische Vorgang über die Weboberfläche oder das Claiming mittels PIN funktionierte hingegen.
- Der Konfigurationspunkt „Unregistered ICMPv6 Flooding“ unter MLD-Snooping war auf Modellen der GS-2328- und GS-2352-Serien ohne Funktion.
- Aufgrund eines zu geringen internen Daten-Buffers wurden zu große TLV-Pakete (Type-Length-Value) verworfen. In der Folge schlug die Authentifizierung eines Clients via 802.1X an einem RADIUS-Server fehl.
- Eine fehlerhafte sFlow-Konfiguration führte dazu, dass ein Switch nach einiger Zeit anstatt „Flow Samples“ nur noch „Counter Samples“ gesendet hat und der sFlow Collector keine Daten mehr empfing.
- Wurde die Weboberfläche des Switches über eine IPv6-Adresse aufgerufen, funktionierte die Anzeige der Online-Hilfe nicht.
- Ein GS-2310(P) lieferte bei Abfrage via SNMP für die CU- und SFP-Ports 9 und 10 jeweils die gleiche Port-ID aus. Nun wird für die CU-Ports die Port-ID 9A und 10A, sowie für die SFTP-Ports 9B und 10B ausgeliefert.

LANCOM GS-23xx Änderungen 3.32.0012 Rel

Neue Features

- Scriptingfähigkeit über die LANCOM Management Cloud
- Hinweis über noch nicht gespeicherte Konfiguration auf der Konfigurationsoberfläche
- Für SSL- und TLS-Konfigurationen sind nun die anzuwendenden SSL- / TLS-Mindestversionen in einer Drop-Down-Liste auswählbar.

Korrekturen / Anpassungen

- Wenn STP auf den Switch-Ports aktiviert war und diese Konfiguration als „Start-Konfiguration“ gespeichert wurde, konnte es nach einem Kaltstart des Switches vorkommen, dass die Angabe der „Uptime“ im Menü „Configuration > Port Status“ mit 2627 Tagen angegeben wurde.
- Ein Hauptgerätepasswort, welches über die LANCOM Management Cloud konfiguriert wurde, war in einem Konfigurations-Export als *.xml-Datei nicht vorhanden.
- Es war keine Online-Hilfe für die Switch-Systeminformationen „LMC pairing state“, „LMC control state“, „Largest free mem block“ und „Free memory“ sowie für die Funktionen „Configuration save“ und „Configuration upload“ vorhanden.
- Bei einem Konfigurations-Export in eine *.xml-Datei fehlten die PoE-Konfigurationsparameter für „Power delay“, „Auto checking“ und „Scheduling“.
- Switch-Ports, bei welchen eine 802.1X Single-/ Multi-Mode Port-Authentifizierung konfiguriert war, wurden nach ca. 4-6 Minuten gesperrt und nach weiteren 4-6 Minuten wieder geöffnet. Der Port-Status wurde immer, auch in den gesperrten Phasen, als „Authorized“ angezeigt.
- Eine automatische Vervollständigung von „show“-Befehlen mit der Tabulator-Taste schlug auf der Kommandozeile aufgrund der Schreibweise des Befehls „show-3rd-party-licenses“ bei allen managed Switches fehl.

- Der Error-String in einer Fehlermeldung wurde auf der Weboberfläche nicht auf die Größe des Meldungsbereichs angepasst.
- Bei Switches des Typs GS-2352x konnte es vorkommen, dass auf bestimmten Ports keine ICMPv6-Pakete übertragen wurden.
- In der Online-Hilfe für die Funktion „Configured link speed“ (im Menü „Port configuration“) fehlten Beschreibungen zu Konfigurationsmöglichkeiten bei unterschiedlichen Switch-Typen.
- Bei Verwendung der Funktion MAC-based authentication für angeschlossene Access Points, kam es bei einem Wechsel der Switch-Ports (durch WLAN-Roaming) zu einem unvermittelten Neustart, wenn die MAC-Adresse der WLAN-Clients im RADIUS-Server hinterlegt war.
- Bei Verwendung mehrerer Switches mit aktiviertem RSTP in einer Ringstruktur und gleichzeitig aktivem DHCP-Snooping kam es bei einer hohen Anzahl an Clients (größer 500) zu einer CPU-Last von 100%.
- Bei aktivem MLD-Snooping kam es zu Kommunikations-Problemen mit IPv6-Paketen, wenn die Netzwerk-Verbindung zum Client getrennt und anschließend wieder hergestellt wurde. Auch konnte es bei Verwendung von IPv6 zu hohen Paketverlusten kommen.
- Allgemeine Stabilitätsverbesserungen

LANCOM GS-23xx Änderungen 3.30.0450 RU4

Neue Features

- Anzeige des aktuellen Speicherverbrauchs auf der Konfigurationsoberfläche bzw. CLI
- Gerätekonfigurationen können nun verschlüsselt exportiert bzw. importiert werden.
- Persistentes Boot- und Eventlog

Korrekturen / Anpassungen

- Obwohl das Kabel LANCOM SFP-DAC10 in den SFP-Informationen richtig angezeigt wurde, kam bei Geräten der LANCOM GS-2310(P)+-Serie kein Link zustande.
- Beim Zurückschreiben einer Switch-Konfiguration von der LMC auf einen Switch wurde das Passwort eines SNMPv3-Benutzers mit 8 Sternen (*****) überschrieben.
- Es konnten gleichzeitig max. 94 unterschiedliche Clients bzw. MAC-Adressen auf das Management des Switches zugreifen. Erfolgte ein Zugriff eines 95. Clients, war die Web-Oberfläche des Switches nicht erreichbar.
- Bei LANCOM SFP-CO1 Kupfer-Modulen wurde im Fall eines LOOP der Portstatus des numerisch kleineren Ports mit „up“ anstatt „down“ angezeigt.
- Wenn in der LANCOM Management Cloud die Zugangsdaten eines Switch-Benutzerkontos erstellt oder bearbeitet wurden, überschrieb die LMC das vergebene Passwort mit dem jeweiligen Benutzernamen. Das Admin-Konto des Switches war davon jedoch nicht betroffen.
- Ein Fehlverhalten in der DHCP-Snooping-Funktion erzeugte eine falsche Verkettung in der internen IP-Liste des Switches, was zu einem LOOP in der Liste führte. In der Folge wurden interne Dienste beim Durchlaufen der Liste endlos ausgeführt, was zu einer Prozessorlast von 100% führte und weitere Prozesse (z.B. den Paketfluss) blockierte.

- › Wenn eine Konfiguration per LMC oder über SNMP in den Switch geschrieben wurde, konnten nicht alle möglichen Aktions-Werte für das ARP-Spoofing gesetzt werden. In der Folge konnte die Konfiguration nicht in den Switch übertragen werden.

LANCOM GS-23xx Änderungen 3.30.0417 RU3

Neue Features

- › Unterstützung für das neue SFP-Kupfermodul LANCOM SFP-CO1
- › Unterstützung für das neue Direct-Attach-Kabel LANCOM SFP-DAC10 für alle Switch-Modelle mit 10G-Ports
- › Neue Funktion „Passwort-Richtlinie“ (Mindestanforderungen an ein sicheres Passwort)

Korrekturen / Anpassungen

- › Es wurde ein Fehlverhalten in Verbindung mit der Management-Erreichbarkeit behoben.
- › Verbesserung der Nutzung der LANCOM Management Cloud
- › Allgemeine Stabilitätsverbesserungen

LANCOM GS-23xx Änderungen 3.30.0324 RU2

Korrekturen / Anpassungen

- › In der LANCOM Management Cloud konnten keine neuen Monitoring-Einträge angelegt werden, wenn die jeweilige Tabelle noch keine Einträge enthielt.
- › Wenn nach einem (Neu)start eines auf DHCP konfigurierten LANCOM Switches kein DHCP-Server im Netzwerk gefunden wurde, scheiterte der Rückfall auf die Fallback-IP-Adresse (172.23.56.250).
- › Wenn bei einem seriellen Zugriff auf einen LANCOM Switch der Trace „lmc-control-data“ ausgeführt wurde, so lieferte dieser fehlerhafte Informationen.

LANCOM GS-23xx Änderungen 3.30.0321 RU1

Korrekturen / Anpassungen

- › Ein von der LANCOM Management Cloud (LMC) getriggertes Firmware-Update funktioniert nun wieder zuverlässig.
- › Über die LANCOM Management Cloud (LMC) konnten die Einträge unter TACACS+ Authentication Server Configuration nicht gelöscht werden.

- Wenn ein Pairing-Vorgang zwischen einem LANCOM Switch des Typs GS-23xx und der LANCOM Management Cloud (LMC) durchgeführt wurde, und das Gerät während des Pairing neu startete, so wurde der ursprünglich ausgeführte Pairing-Vorgang nach dem Neustart des Gerätes nicht automatisch erneut angestossen.
- Wenn bei einem LANCOM GS-2352(P) das Management VLAN eine ID ungleich 0 aufwies, konnten diese Geräte bei aktiviertem IGMP-Snooping nicht mit der Gerätesuche von LANconfig gefunden werden.
- Obwohl im LLDP mehrere IPv6-Management-Adressen angekündigt wurden, zeigte der Dialog „LLDP > LLDP Neighbours“ nur die erste IPv6 Management Adresse an.
- Eine zweite über LLDP gelernte Management-Adresse eines anderen Device konnte nicht als Link aufgerufen werden.
- Die SNMP-Ausgabe von „dot1qVlanStaticEgressPorts“ der Q-Bridge MIB erfolgte in dezimaler Form. Dies wurde nun in eine SNMP-Ausgabe als Octett String geändert.
- Ein Abruf des Port-Status über HTTP/S unter Security -> Port Security -> Port Status -> „Port“ führte zu einer Nichtverfügbarkeit des Switch-Managements (über die Management-IP), wenn die Funktion aktiviert und auf dem aufgerufenen Port viele MAC-Adressen gelistet waren.
- Das Eintragen eines Hostnamens unter ‚TACACS+ Authentication Server Configuration‘ führte nach Bestätigung der Änderung zu einem unvermittelten Neustarts des Switches.

LANCOM GS-23xx Änderungen 3.30.0204 Rel

Korrekturen / Anpassungen

- Mögliche Speicherverluste bei der Verwendung von SNMP und SSH wurden behoben.
- Zufällige Verbindungsabbrüche bei der Verwendung von SSH wurden behoben.
- Die Aktivierung von Voice-VLAN führt nun nicht mehr zur statischen Eintragung dynamischer
- Mac- Adressen in der Mac-Adress-Table

LANCOM GS-23xx Änderungen 3.30.0115 RC1

Neue Features

- Unterstützung der LANCOM Management Cloud (LMC)
- Es ist nun möglich, einen Kaltstart des Gerätes sowohl über die Konfigurationsoberfläche, als auch über die Kommandozeile durchzuführen.
- Im Syslog können jetzt bis zu 1000 Syslog-Meldungen gespeichert werden. Die Einträge der Syslog-Tabelle können nach der Uhrzeit sortiert werden.
- Durch eine Erweiterung der SNMP-MIB Struktur (private MIB) können jetzt AAA, IGMP snooping, SNMPv2/v3, NAS, sowie Private based VLAN und MAC based VLAN konfiguriert werden.
- Im Menü Voice VLAN wurde in der OUI-Tabelle der Hersteller Innovaphone hinzugefügt.

Korrekturen / Anpassungen

- › Die Konfigurationsoberfläche wird bei einer Bildschirmauflösung von 2560 x 1440 Pixeln wieder korrekt angezeigt.
- › Eine mit Keepalive konfigurierte SSH-Verbindung führt nicht mehr zu einem Neustart des Gerätes.

LANCOM GS-23xx Änderungen 3.22.0003 Rel

Neue Features

- › Unterstützung von AES 128 für SNMPv3
- › SNMP Get Community können jetzt (de-)aktiviert werden.
- › Das NTP Synchronisationsintervall kann nun konfiguriert werden.
- › Auf der CLI kann für einen Neustart des Switches nun eine Zeit mit angegeben werden.

Korrekturen / Anpassungen

- › Die LLDP Nachbarn werden nun mit der korrekten IPv6-Adresse angezeigt.
- › Es wurde ein Fehler behoben, bei dem der Switch nach einem Neustart manchmal nicht mehr erreichbar war.
- › Ein Problem mit der DHCP Option 43 wurde behoben.
- › Ist die IPv6 Autokonfiguration eingeschaltet, wird die IPv6-Adresse automatisch aktualisiert wenn sich das Präfix ändert.
- › Wird die Authentifizierung über Telnet verboten, so wird nun der Port komplett deaktiviert und nicht nur die Anmeldung verboten.

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 3.17 Rel

Neue Features

- › Es können nun fünf weitere SNMP GET Communities konfiguriert werden.
- › Die SSL Zertifikate werden nun mit SHA-2 (SHA-512) signiert.
- › Aktualisierung der Dropbear SSH Version

Korrekturen / Anpassungen

- › Im Autonegotiation-Modus werden nun auch vieradrige Netzkabel unterstützt.
- › Nach einem Firmwareupgrade muss kein „cert-renew“ für den HTTPS Zugriff über Firefox ausgeführt werden.
- › Über die CLI kann die Portgeschwindigkeit von „10Mbps half duplex“ oder „100Mbps half duplex“ auf „Auto“ geändert werden.
- › Verbesserung der Easy Port und SCP Funktionalität

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 3.10 Rel

Neue Features

- › Es kann nun auf Basis von fehlerhaften Logins eine automatische und protokollbasierte Zugriffssperre konfiguriert werden.
- › XML-Konfigurationsdateien werden jetzt mit einem zusätzlichen Header gespeichert. Dieser beinhaltet Informationen zum Gerätetyp, Export-Datum, Firmware-Version und Seriennummer.
- › Die IPv6 Informationen in den Systeminformationen wurden erweitert.
- › Die NTP Konfiguration unterstützt nun auch Domännennamen.
- › In den QoS Einstellungen kann nun konfiguriert werden für welche Quell- und Ziel-IP priorisiert werden soll.
- › Das IPv6 Präfix hat jetzt eine Default-Länge von 64 Bit.
- › Die Passwortlänge des RADIUS Shared Secret wurde auf 64 Zeichen erhöht.
- › Easy Port unterstützt nun Multi-VLAN und es können eigene Templates angelegt werden.
- › Unterstützung von DHCP Option 43
- › Verbesserungen der DHCP Relay-Funktion
- › Unterstützung des LSR
- › Unterstützung von RSA 2048 bei SSH und HTTPS Zugriff.
- › DES-basierte Verschlüsselungen wurden entfernt.
- › Unterstützung von ARP Spoofing
- › Der DHCP-Relay-Agent unterstützt nun mehrere VLAN, Port und Access-Groups.
- › Die GIADDR für die DHCP Relay Funktion kann konfiguriert werden.
- › 5 weitere SNMP Communities wurden hinzugefügt.
- › Verbesserte Generierung des HTTPS Zertifikats.
- › Unterstützung von DH 2048 Bit

Korrekturen / Anpassungen

- › Der Switch sendet nun ein Stop-Accounting-Status-Type wenn das Accounting beendet ist.
- › Der Switch sendet TFTP-Accounting-Informationen wenn die TACACS+-Authentifizierung aktiviert ist.
- › MAC-basierte Authentifizierung über 802.1X funktioniert wieder korrekt.
- › Die Static Trunk Konfiguration wird beim Export / Import einer Konfigurationsdatei wieder mit ex- / importiert.
- › Die Port-Beschreibung kann über die CLI bearbeitet bzw. entfernt werden
- › Es wurde ein Fehler behoben, der dazu führte, dass der Switch neustartete wenn IGMP Pakete weitergeleitet wurden und ein Link entfernt wurde.
- › Die PVID kann über die CLI wieder geändert werden.
- › Der Switch startet nicht mehr neu wenn er ein DHCP Offer- / Ack-Paket größer 576 bytes empfängt.
- › Zugriff mit Firefox v39.0 und höher über HTTPS funktioniert wieder.

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P Änderungen 2.83 Rel

Neue Features

- › Die Online Hilfe wurde überarbeitet.
- › In den Systeminformationen wird nun auch die Hardwareversion angezeigt.
- › Die Konfiguration und Firmware kann nun auch über SCP eingespielt werden.
- › Unterstützung weiterer Radius Attribute beim Login/Logout
- › Die Defaultwerte der Zeit Konfiguration wurden angepasst.
- › Die HTTPS Zertifikate wurden verbessert.
- › Auf der Konsole kann mit dem Befehl „cert-renew“ ein neues HTTPS Zertifikat mit eindeutiger Seriennummer erzeugt werden.
- › Der Zugriff über TFTP kann konfiguriert werden.
- › Die LANCOM GS-2352 und GS-2352P unterstützen nun die folgenden 10GB SFP Direct-Attach-Kabel:
 - HP SFP+ Direct Attach 1m J9281B
 - D-link DEM-cb300S P3400XA03000-A
 - Intel Ethernet SFP+ Twinaxial Cable XDACBL3M - Twinaxial-Kabel - SFP+ (M)
- › Der Gerätenamen wird im Browsertab angezeigt.

Korrekturen / Anpassungen

- › Ein Client bekommt bei aktiviertem DHCP Snooping in einer PXE Umgebung wieder eine Adresse zugewiesen.
- › An einem per 802.1x gesicherten Port bekommt man ohne Authentifizierung keine Adresse mehr zugewiesen.
- › Das Aktivieren von DHCP Snooping führt nicht mehr zu einem Absturz.
- › Die Verbindung zu einem TACACS+ Server wird bei aktiviertem Accounting nicht mehr getrennt, wenn mehrere Befehle ausgeführt werden.
- › Der Zugriff auf weitere Switches per Single IP über HTTPS wurde korrigiert.
- › Wenn der IPv4 und IPv6 Client aktiviert ist und der Gerätenamen mehr als 254 Zeichen enthält, führt dies nicht mehr dazu, dass unzählige Router Solicitations pro Sekunde verschickt werden.
- › Melden sich mehrere Clients an einem mittels 802.1x gesicherten Port an, führt dies nicht mehr zu einem Absturz.
- › Die Konfiguration kann wieder über LANconfig als XML im- /exportiert werden.
- › Enthält Passwort unzulässige Zeichen, führt dies zu einer Fehlermeldung.
- › Der Down- und Upload der Konfiguration über TFTP kann nur noch von einem User durchgeführt werden, der die dazu konfigurierte Berechtigungsstufe hat.
- › Der TFTP Down- und Upload funktioniert auch wenn das erste Zeichen des Passworts ein „@“ ist.
- › Beim Versand von E-Mails wird die Einstellung für Sommer- /Winterzeit mit berücksichtigt.

LANCOM GS-2326(P) / GS-2352(P) Änderungen 2.52 Rel

Neue Features

- › Ist der Zugriff auf den Switch mit TACACS+ oder RADIUS Authentifizierung abgesichert, so wird dies auf der Weboberfläche angezeigt.
- › Die Private MIB wurde um die PoE und VLAN Port Konfiguration erweitert.
- › Unterstützung für SSL Verschlüsselung mit 1024 Bit
- › Der Default Wert für den VLAN Port wurde auf „C-port“ geändert.
- › Die Hintergrundfarbe der Weboberfläche wurde angepasst.
- › Bei einem Firmwareupdate wird für eine korrekte Anzeige in LANconfig ein Status-Code zurückgegeben.

Korrekturen / Anpassungen

- › Zugriff über einen LACP Link mit IPv6 ist nach einem Reboot möglich
- › Die Beschriftung des Seriennummern-Feldes wurde korrigiert.
- › Werden bei TFTP Zugriff keine Benutzerinformationen mitgegeben, wird ein entsprechender Fehlercode für LANconfig zurückgegeben.
- › Es wurden Hilfen für TACACS+ Authorization, Accounting Configuration und Traffic Class hinzugefügt.
- › Der Navigationsbereich wird im Internet Explorer 10 wieder angezeigt.
- › Angepasste Hilfe für die ACL Konfiguration.
- › LLDP-MED Einstellungen können über die MIB abgerufen werden.
- › Ein PXE Boot Client bekommt eine IP-Adresse, wenn DHCP Snooping aktiviert ist.
- › Die Hilfe für die Seriennummer wurde korrigiert.
- › Der Export und Import der Konfiguration berücksichtigt nun alle Parameter.
- › Ist DHCP Snooping auf einem Trusted Ethernet Port erlaubt, werden DHCP Pakete auf den Ports 66-89 und 4011 erlaubt.
- › Der Switch wartet bis zu 15 Minuten auf die Zuweisung einer IP-Adresse durch einen DHCP Server, bevor er auf seine Default IP-Adresse zurückfällt.
- › Der DHCP Hostname wurde angepasst.
- › Die Hilfe für die Circuit- und Remote ID wurden korrigiert.
- › Die MIB gibt den korrekten Wert für „pethPsePortDetectionStatus“ zurück.
- › Die Default Werte der IPv6 Konfiguration wurden korrigiert.
- › Der Default Wert für das Ändern der Berechtigungsstufen wurde auf das Privilege Level 15 angehoben.
- › Ist ein Loop zwischen 802.1x konfigurierten Ports gesteckt, bootet der Switch nicht mehr.
- › Bei der SMTP Konfiguration wird der Empfänger nur noch einmal eingetragen.
- › Der Konfigurationsimport funktioniert auch mit langer VLAN Bezeichnung.

LANCOM GS-2326(P) / GS-2352 Änderungen 2.26 Rel

Korrekturen / Anpassungen

- › Die SNMPv3 Trap Host Konfigurationsanzeige wird wieder korrekt angezeigt, nachdem ein SNMP Kommando über die Kommandozeile ausgeführt wurde.
- › ACL funktioniert auch wenn ARP Pakete empfangen werden.
- › Das Passwort wird nicht mehr entfernt, wenn der Systemname geändert wird.
- › Der Modellname wird korrekt angezeigt, wenn dieser über SNMPc abgerufen wird.
- › Verbesserte Reboot/Restore Schaltfläche
- › Die Pfadkosten bei gleichzeitiger Verwendung von STP und Aggregation werden nun korrekt ermittelt.
- › Auf einem Windows 2008 Server wird nun die MAC Adresse des Switches angezeigt.
- › Alle Geräte, bei denen die ersten vier Byte der MAC Adresse identisch sind, werden nun angezeigt.
- › Bei abgeschaltetem Port werden keine Trap Events mehr verschickt.
- › Easy Port: Der Traffic Class Wert kann auch für IP-CAM und WIFI-AP geändert werden.
- › Easy Port: Es gibt eine Rückmeldung, wenn der Apply Button gedrückt wurde.
- › Easy Port: Wird Port Security auf einem Port eingeschaltet, wird diese auch global aktiviert.
- › Easy Port: Bei IP-CAM und WIFI AP wird anhand der VLAN ID eine VLAN Gruppe mit den ausgewählten Ports gebildet.
- › Auf der Kommandozeile wird der Modellname angezeigt.
- › Es wird kein Reboot mehr ausgelöst, wenn per SSH über LANconfig auf den Switch zugegriffen wird.
- › Die Antwortzeit beim Scan der Ethernet- und PoE Ports mittels LANmonitor wurde verbessert.
- › Anpassung im NTP Protokoll: die Zeitabfrage funktioniert nun zuverlässig
- › Beim Passwort können nun auch „%“ und „+“ Zeichen verwendet werden.

LANCOM GS-2326 / GS-2352 Änderungen 1.65 Rel

Korrekturen / Anpassungen

- › Ping-Antwortzeiten des Switches wurden verbessert
- › Änderungen der Systembeschreibungparameter können nicht mehr zur Rücksetzung des Gerätepasswortes auf den Default führen.
- › Optimierungen der 10Gbit Ports verbessern das Pakethandling von Paketen mit hoher Laufzeit.
- › Multicastpakete in einer Ring-Topologie führen nicht mehr dazu, dass bei mehrfachem Ziehen/Stecken des Kabels der Zugriff auf das Management verloren gehen kann.
- › Ein Problem wurde behoben, welches dazu führen konnte, dass die MIB-Datei nicht vollständig ausgelesen wurde.
- › Ein SNMP-Walk kann jetzt jederzeit fehlerfrei durchgeführt werden
- › Ein Problem beim Import von Konfigurationsdateien wurde behoben.
- › Die 802.1x Authentifizierung bei Nutzung eines Windows 2008 Servers als Radius-Server wurde verbessert.

LANCOM GS-2326 / GS-2352 Änderungen 1.48 RC1

Korrekturen / Anpassungen

- › Wiederholtes Ein-Ausschalten des Ports konnte zu Verbindungsverlust führen
- › Problem bei der Geschwindigkeitserkennung im Automodus auf den 10G SFP Ports behoben
- › LACP Stabilität verbessert
- › Anzeige der IPv6 Link-Local-Adresse angepasst
- › Ping Antwortverhalten auf die Link-Local-Adresse korrigiert
- › Fehlerhafte Anzeige der Syslog Konfiguration berichtigt
- › Verbesserte Systemstabilität bei gleichzeitiger Konfiguration von STP und LACP
- › Anzeige im Web Interface nach Speichern der User Konfiguration angepasst
- › Es kann nun eine SNMP Trap-Server IP Adresse konfiguriert werden
- › Anzeige nach Firmwareupload oder Neustart über das Webinterface korrigiert

4. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Support-Hinweise & bekannte Einschränkungen

Aktuelle Support-Hinweise und bekannte Einschränkungen zur aktuellen LCOS SX-Version finden Sie im Download-Bereich unserer Webseite: [Allgemeine Support-Hinweise](#)