

LANCOM Release Notes

LCOS

8.84 SU11

Copyright (c) 2002-2019 LANCOM Systems GmbH, Würselen (Germany)

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

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

05.11.2019, CBuersch

Inhaltsübersicht

1. Einleitung	2
2. Gerätespezifische Kompatibilität zu LCOS 8.84	2
3. Historie LCOS 8.84	4
LCOS Änderungen 8.84.0309 SU11	4
LCOS Änderungen 8.84.0308 SU10	5
LCOS Änderungen 8.84.0289 SU9	5
LCOS Änderungen 8.84.0267 RU8	6
LCOS Änderungen 8.84.0262 RU7	6
LCOS Änderungen 8.84.0244 RU6	7
LCOS Änderungen 8.84.0231 RU5	7
LCOS Änderungen 8.84.0193 RU3	9
LCOS Änderungen 8.84.0177 RU2	9
LCOS Änderungen 8.84.0142 RU1	11
LCOS Änderungen 8.84.0132 Rel	11
LCOS Änderungen 8.84.0103 RC1	11
LCOS Änderungen 8.82.0123 RU2	13
LCOS Änderungen 8.82.0100 RU1	14
LCOS Änderungen 8.82.0089 Rel	15
LCOS Änderungen 8.82.0067 RC2	15
LCOS Änderungen 8.82.0051 RC1	16
LCOS Änderungen 8.80.0159 RU1	17
LCOS Änderungen 8.80.0157 RU1	17

4. Allgemeine Hinweise	18
Haftungsausschluss	18
Sichern der aktuellen Konfiguration	18
Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes	18

1. Einleitung

LCOS („LANCOM Operating System“) ist das bewährte LANCOM Betriebssystem für Router, Access Points und WLAN-Controller. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS-Version für LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 8.84 SU11 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 4 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite

<https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/>

2. Gerätespezifische Kompatibilität zu LCOS 8.84

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten.

Auch für Geräte, die keine aktuelle LCOS-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstützte LCOS-Version für Ihr Gerät finden Sie unter

<https://www.lancom-systems.de/produkte/firmware/lifecycle-management/produkttabellen/>

Mit LCOS 8.50 entfällt die Unterstützung für folgende Geräte

- > LANCOM 1811 Wireless
- > LANCOM 1721 VPN

Bei den nachfolgenden Geräten entfällt ab LCOS 8.60 in WEBconfig die an LANconfig angelehnte Ansicht „Konfiguration“

- > LANCOM L-310
- > LANCOM L-305
- > LANCOM L-54 dual Wireless
- > T-Systems Business LAN R800+

Verwenden Sie stattdessen entweder LANconfig, oder nutzen Sie in WEBconfig den Konfigurationsbereich „LCOS-Menübaum“.

Mit LCOS 8.80 entfällt die Unterstützung für folgende Geräte

- > LANCOM L-54 Wireless (kleiner Hardwarerelease E)
- > LANCOM L-54 dual Wireless (kleiner Hardwarerelease G)
- > LANCOM OAP-54-1 Wireless

Mit LCOS 8.82 entfällt die Unterstützung für folgende Geräte

- > LANCOM XAP Wireless
- > LANCOM L-305 / L-310 Wireless
- > LANCOM L-54 dual Wireless

Mit LCOS 8.84 entfällt die Unterstützung für folgende Geräte

- > Telekom R800+
- > LANCOM 821+
- > LANCOM 1611+
- > LANCOM 1711
- > LANCOM 1821n

3. Historie LCOS 8.84

LCOS Änderungen 8.84.0309 SU11

Korrekturen / Anpassungen

Allgemein

- > Es wurde ein potentiell sicherheitsrelevantes Problem auf LANCOM Routern in Verbindung mit IPv6 behoben. Dieses kann auftreten, wenn IPv6-Netze über IPSec (IKEv1 oder IKEv2) verbunden werden und gleichzeitig eine IPv6-Internet-Verbindung verwendet wird. In diesem Fall wird eine Aktualisierung auf die aktuelle LCOS-Version dringend empfohlen. Der Fehler ist in den folgenden LCOS-Versionen behoben:
 - > LCOS 10.32 SU3
 - > LCOS 10.20 SU9
 - > LCOS 10.12 SU14
 - > LCOS 9.24 SU12
 - > LCOS 9.00 SU8
 - > LCOS 8.84 SU11
- > SSL/TLS-Handshake-Pakete können in seltenen Fällen so groß werden, dass diese über mehrere Records verteilt werden müssen. Es wurde jetzt ein SSL/TLS-Reassembler implementiert, der die Pakete wieder zusammensetzt.
- > Auf der Konsole konnten mit dem LL2M-Broadcast-Befehl ,ll2mdetect - b' keine LANCOM Geräte gefunden werden.

LCOS Änderungen 8.84.0308 SU10

Korrekturen / Anpassungen

Allgemein

- › Es wurde eine Sicherheitslücke im WPA2-Verfahren (KRACK-Attacke) im Zusammenhang mit der Nutzung von Punkt-zu-Punkt-Strecken mit 802.11a/b/g/n-WLAN-Modulen behoben:

CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake

CVE-2017-13080: reinstallation of the group key in the Group Key handshake

Der mit 802.11a/b/g/n-WLAN-Modulen betriebene WLAN-Client-Modus / WLAN-Station-Mode ist nicht betroffen.

Hinweis

- › Von den folgenden WPA2-Sicherheitslücken (KRACK-Attacke) ist das LCOS **NICHT** betroffen:

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake

CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake

CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

CVE-2017-13078: reinstallation of the group key in the Four-way handshake

CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

- › Von den folgenden WPA2-Sicherheitslücken (KRACK-Attacke) ist das LCOS nur in Zusammenhang mit der Nutzung von 802.11r (Fast-Roaming) betroffen, was von dieser LCOS-Version nicht unterstützt wird:

CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it

LCOS Änderungen 8.84.0289 SU9

Korrekturen/Anpassungen

Network Connectivity

- › Falls das Gerät keine individuellen SSL-/SSH-Keys hat, werden diese einmalig erzeugt.
- › Unterstützung für SHA-256 im SSL-Gerätezertifikat der Webconfig
- › Verwendung von 2048 Bit Diffie-Hellman bei TLS Handshake

LCOS Änderungen 8.84.0267 RU8

Neue Features:

Network Connectivity:

- › Das Mobilfunknetz kann jetzt anhand der Signalstärke ausgewählt werden.

LCOS Änderungen 8.84.0262 RU7

Korrekturen/Anpassungen

Network Connectivity

- › Bei sich überschneidenden Netzen werden Antwortpakete an das korrekte Netz weitergeleitet.
- › Eine vom DHCP-Server vergebene Adresse wird nur noch gegen das Netzwerk geprüft, über welches die DHCP-Anfrage hereingekommen ist.
- › Es wurde ein Fehler behoben, der dazu führte, dass bei einem Gespräch von einem ISDN Telefon über eine All-IP Leitung die Sprachübertragung abgebrochen ist.
- › Die Telekom Sprachbox kann wieder abgerufen werden.
- › Der Rufnummertyp der Called-Party-Number wird für ISDN-Benutzer nun passend zur übertragenen Rufnummer gesetzt.
- › Es wurde ein Problem behoben, welches dazu führte, dass ADSL Down- und Upstream nicht angezeigt wurden.
- › Ein LANCOM antwortet nun bei einem DNS Lookup auf seinen Namen wieder mit seiner IP-Adresse.
- › Es wurde ein Fehler behoben, der dazu führte, dass nach einem VPN Phase 2 Soft Timeout keine neue Phase 2 SA aufgebaut wurde.
- › Das Überwachungsintervall für SIP Leitungen wird wieder korrekt behandelt.
- › SIP-Leitungen registrieren sich auch wenn SIP-ALG aktiviert ist.
- › Ein PPTP Verbindungsaufbau funktioniert auch wenn das Ziel eine IPSec Backupverbindung ist.
- › Die Namen der ADSL Schnittstellen wurden in der MIB angepasst.

WLAN

- › Stabilitätsverbesserungen für Szenarien mit vielen WLAN-Clients.
- › Es wurde ein Problem behoben, bei dem WLAN-Clients eingebucht waren, aber keine Datenübertragung möglich war.
- › Verhinderung von doppelten MAC-Adresseinträgen in der Stationstabelle.

- › Ein Problem mit AR93xx basierten WLAN-Modulen bei TKIP-verschlüsselten Netzen wurde behoben.

LCOS Änderungen 8.84.0244 RU6

Korrekturen/Anpassungen

Network Connectivity

- › Verbesserte Unterstützung der VoIP-Router für Double-Challenge-Authentifizierung.
- › ADSL Sub Interfaces werden in der MIB des 1781A-3G angezeigt.
- › Ein Problem mit dem VPN Load Balancer wurde behoben.
- › Ein Problem mit der Bandbreitenreservierung wurde behoben.
- › Auf der CLI ist es nicht mehr möglich, mehrere DNS-Einträge für den gleichen Namen anzulegen.

WLAN

- › Die Sendeleistung von abg WLAN Modulen wurde angepasst.

LCOS Änderungen 8.84.0231 RU5

Korrekturen/Anpassungen

Network Connectivity

- › Treten während einer PPP-Verhandlung Fehler auf, wird eine Backupverbindung immer aufgebaut wenn die Gegenstelle mit einer Haltezeit von 9999 konfiguriert ist.
- › Propagierung zusätzlicher Routen per RIP angepasst.
- › Ein Problem mit einer SNMP Abfrage wurde behoben.
- › Das CLI Kommando „who“ gibt jetzt die korrekte Uhrzeit mit an.
- › Ein Problem wurde behoben, bei dem mit LANconfig offline erstellte Konfigurationen nicht mehr über WEBconfig eingespielt werden konnten.
- › Ein Problem beim Versand von SMS wurde behoben.
- › Der RTP Timestamp wird bei RTP Events im Callmanager korrekt gesetzt.
- › Wird das WWAN Modul im LCOS abgeschaltet, wird die Verbindung mit abgebaut.

WLAN

- › Die Ablaufarten werden bei Verwendung von E-Mail2SMS wieder korrekt herangezogen.
- › Problem im Block-Ack-Handling bei verschiedenen WLAN-Clients behoben.
- › Verbesserung der WLAN-Sendeleistung im 2.4 Ghz Band.

LCOS Änderungen 8.84.0193 RU3

Neue Features

Network Connectivity

- > LCOSCap und RPsap werden automatisch beendet wenn ein Firmwareupdate durchgeführt wird.
- > Unterstützung des 1781VA-4G

Korrekturen/Anpassungen

WLAN

- > Wenn RPsap verwendet wird, werden auch Authentication und Association Frames mit aufgezeichnet.
- > Verbesserungen im Public Spot

Network Connectivity

- > Der DHCP Server ignoriert Pakete mit ungültiger bzw. falscher Checksumme.
- > Es wurde ein Fehler behoben, der zu einer nicht funktionierenden DNS Weiterleitung führte.
- > Verbesserungen im SIP-ALG
- > Bei Verwendung des Volumenbudgets wird ein Monatswechsel berücksichtigt.

LCOS Änderungen 8.84.0177 RU2

Neue Features

Network Connectivity

- > Konfigurierbares RIP Output Delay
- > RIP-Responses als Antwort auf einen RIP-Request werden nun an den Quellport des RIP-Requests geschickt (RFC 2453)
- > Es ist jetzt möglich, die SIM-PIN zu ändern
- > Im Content Filter wird der FQDN der per HTTPS angesteuerten Seite aus dem Serverzertifikat entnommen
- > Unterstützung von VDSL Vectoring für ‚overISDN‘ LANCOM Geräte

Korrekturen/Anpassungen

WLAN

- › Kein Neustart des Access Points bei der Druckersuche über die Android App „Page Scope Mobile“
- › Fehlerfreies Public Spot Login mit italienischer und spanischer Browsersprache
- › Keine Endlosschleife beim Beenden des Spectral Scan
- › Bugfix im RADIUS Protokollhandling
- › Korrigierte Ausgabe im PMS-Trace
- › Überarbeitete PMS Accounting Plus Option
- › Überarbeitetes Public Spot Login
- › Public Spot Login-Text für das LANCOM 1823 freigeschaltet
- › Korrekturen im XML-Interface für das Re-Login am Public Spot

Network Connectivity

- › Die Backupverbindung für das Event „Volumen-Budget überschritten“ wird auch aufgebaut, wenn für diese kein Keepalive gesetzt ist.
- › Ein manuell gesetzter, alternativer SMTP Port wird wieder berücksichtigt.
- › Hardware-NAT wurde für PPPoE Gegenstellen deaktiviert.
- › Verbesserungen im IKE Speichermanagement
- › Überarbeitete Kanalauswahl im Loadbalancer
- › CLI: Überarbeitete Statusanzeige im VPN-Menü
- › Überarbeitete SIM-Karten Erkennung
- › Korrigiertes MTU-Handling im IPv6
- › Padding-Bytes werden im MLPP wieder berücksichtigt
- › Behandlung des Link End Record in der FIAS Schnittstelle angepasst
- › Anpassungen in der DH-Vorbereitung
- › LANCAPI: Bessere Unterstützung von DDI
- › LANCAPI: Überarbeitung im Handling der LANCAPI-MSN
- › LANCAPI: Die LANCAPI lehnt einen ankommenden Ruf ab, wenn sie weiß, daß niemand diesen entgegennehmen wird.

LCOS Änderungen 8.84.0142 RU1

Neue Features

Network Connectivity

- > Limitierung der SMS Sendeversuche auf Vorgabe 2 implementiert
- > Syslog Meldung bei fehlgeschlagenem SMS Versand

Korrekturen/Anpassungen

- > SSH „Keepalive“ lässt sich nun auf der CLI setzen

LCOS Änderungen 8.84.0132 Rel

Neue Features

Network Connectivity

- > Implementation einer X.25 Bridge
- > Konfigurationsmöglichkeit weiterer SNMP-Communities

Korrekturen/Anpassungen

WLAN

- > Wird die IP-Verwaltung der Accesspoints vom WLC statisch durchgeführt, wird beim Löschen der IP-Adresse der DHCP-Server wieder aktiviert.
- > Die RADIUS-Accounting Daten werden bei Verwendung der XML-Schnittstelle vollständig übermittelt.

VoIP

- > Die vom SIP-ALG verwendete WAN-Adresse wird im Status richtig ausgegeben.

Network Connectivity

- > Wird die TACACS+-Autorisierung verwendet, wird auch bei einer SSH-Verbindung kein ReadOnly-Zugriff angezeigt, da der TACACS+-Server die Rechte-Verwaltung der Befehle übernimmt.
- > Gelesene SMS-Nachrichten können als „ungelesen“ markiert werden.
- > Accounting-Daten werden wieder vollständig gesammelt.
- > Die vom RADIUS-Server gemeldeten Zugriffsrechte werden nun richtig ausgewertet.
- > OCSP ist auch auf einem LANCOM 1681V verfügbar.

LCOS Änderungen 8.84.0103 RC1

Neue Features

WLAN

- › RADIUS-Anfragen an den MAC-Address-Check-Provider werden zwischengespeichert, um unnötige Anfragen zu vermeiden.
- › 802.11u (Hotspot 2.0) kann über den WLAN Controller konfiguriert werden.
- › Besserer WLAN-Durchsatz durch Immunität gegen Störsignale durch Adaptive Noise Immunity
- › Benutzerkonten können in der RADIUS-Tabelle einzeln (de-)aktiviert werden.
- › Das LANCOM erkennt, ob ein Querier im Netzwerk vorhanden ist und schaltet ggf. IGMP-Snooping automatisch ein.
- › Multi-/Broadcasts können im WLAN mit der niedrigsten genutzten Rate aller eingebuchter WLAN Clients verschickt werden.
- › Beschleunigung des WLAN-Roamings bei der Nutzung von WPA2-Enterprise durch OKC
- › Es kann eine Public Spot Fehlerseite angezeigt werden, wenn die WAN-Verbindung gestört ist.
- › Bei der Public Spot Anmeldung via Voucher kann eine AGB Bestätigung aktiviert werden.
- › Die Smart Ticket Webseiten können individualisiert werden.
- › Erweiterung Public Spot Seiten um weitere Sprachen.
- › Bei Nutzung von Public Spot kann der Benutzer nachträglich die Sitzungsinformationsseite öffnen.
- › Bei einer fehlgeschlagenen Public Spot Anmeldung wird das Feld „Benutzername“ nicht mehr zurückgesetzt.
- › Bei der Verwendung von Smart Ticket kann der Benutzer die Mobilfunknummer im beliebigen Format angeben.
- › Smart Ticket kann die SMS direkt über das LANCOM Mobilfunkmodul verschicken.
- › DHCP-Antworten können im WLAN von Broadcasts in Unicasts gewandelt werden.
- › In einem Public Spot Template kann benutzerspezifischer HTML Code verwendet werden. Dieser wird benutzerabhängig auf dem Voucher angezeigt.
- › Für die Public Spot Authentifizierung kann die LAN-MAC, die LANCOM IP sowie die Client-IP in der URL übergeben werden.

Network Connectivity

- › Anzeige des Datenvolumens für WAN-Verbindungen.
- › DSL Sync Informationen werden im SYSLOG protokolliert
- › Detaillierte Informationen zu Mobilfunkverbindungen werden im SYSLOG protokolliert.
- › Bei IPv6 WAN-Verbindungen mit einem /64 Präfix kann dieses unverändert ins LAN weitergeleitet werden.
- › Unterstützung des UMTS-Sticks Web'n'Walk Fusion III
- › Die zu nutzenden LTE-Frequenzbänder können fest eingestellt werden.
- › ARF-Netzwerke mit gleichem IP-Adresskreis können über Proxy ARP miteinander verbunden werden.
- › Empfang und Versand von SMS über das LANCOM Mobilfunkmodul
- › Implementation eines Rollout-Assistenten
- › In der Aktionstabelle können auch IPv6-Adressen verarbeitet werden

- Der LANCOM SMTP Client unterstützt auch verschlüsselte Verbindungen (TLS/STARTTLS).
- Eine RADIUS Authentisierung kann für das Gerätelogin genutzt werden.
- Das LANCOM erzeugt nach einem Systemreset automatisch einen SSH-Schlüssel.
- Informationen zu WAN-Verbindungen, die über IPoE/DHCPoE hergestellt werden, werden im SYSLOG protokolliert.
- Geräteinformationen werden nicht mehr im HTTP Header übertragen.
- Die Aktionstabelle wurde um das Routing Tag erweitert.
- Der SMS Versand kann über einen entsprechenden HTTP Aufruf erfolgen, bei dem Mobilfunknummer und Text als Parameter übergeben werden.

Korrekturen/Anpassungen

WLAN

- Access Points in gerouteten Subnetzen verbinden sich nach einem Gerätereustart wieder mit dem WLC.
- Ein Traceroute über eine getaggte Verbindung wird nun aus dem richtigen ARF-Netz beantwortet.
- Neue Public Spot Benutzer können mit Hilfe des Einrichtungsassistenten auch schnell hintereinander angelegt werden.
- Die Anmeldung eines Public Spot Benutzers ohne Browser (WISPr) funktioniert nun in Version 1.0 und 2.0
- Nachdem sich der Benutzer vom Public Spot abgemeldet hat, kann er auch die zuletzt aufgerufene Internetseite nicht weiter nutzen.

VoIP

- Verbindet ein externer ISDN-Teilnehmer das Gespräch an eine weitere Gegenstelle, funktioniert diese Verbindung nun in beide Richtungen.
- Der SIP ALG behandelt nun auch Kurzformen im SIP Header korrekt.

Network Connectivity

- Es erscheinen keine unnötigen Zertifikatsfehler mehr im SYSLOG
- Die VPN Lastbegrenzung für gleichzeitige Tunnelaufbauten funktioniert nun auch bei Aggressive-Mode Verbindungen.
- IPv6-Präfixänderungen auf dem WAN-Interface werden auch im LAN entsprechend berücksichtigt.
- Bei aktiven DNS-Forwarder und deaktiviertem DNS-Server antwortet das LANCOM auf DNS-Anfragen über eine maskierte Default-Route mit einem „Port unreachable“.
- Der CLI-Befehl „show vpn“ liefert nun immer die komplette Ausgabe der VPN Regeln.
- NAT-T wird in der IPv6-Firewall Defaultkonfiguration berücksichtigt.
- Der CLI-Befehl „sshkeygen“ kann mit dem Parameter „-q“ auch in Skripten verwendet werden.

LCOS Änderungen 8.82.0123 RU2

Korrekturen/Anpassungen

Network Connectivity

- › Schnellere Initialisierung der internen 3G/4G Mobilfunkkarte nach dem Start.

LCOS Änderungen 8.82.0100 RU1

Korrekturen/Anpassungen

WLAN

- › Bei der Konfiguration von Public Spot Email/SMS Ländercodes kommt es nicht mehr zu einem Routerneustart.
- › Greift ein nicht angemeldeter Public Spot Client auf eine HTTPS-Seite zu, wird das hierzu erzeugte SSL-Zertifikat später wieder entfernt. Somit wird ein Neustart aufgrund von Speichermangel vermieden.
- › Die Anmeldung eines Public Spot Benutzers ohne Browser (WISPr) kann nun auch mit dem Windows 8 Client genutzt werden.
- › Werden Multi- und Broadcasts auf einer WLAN SSID unterdrückt, kann ein Client dennoch via DHCP eine Adresse beziehen.

VoIP

- › Verbesserte Unterstützung eines nicht T.38 fähigen Faxes an einer T.38 unterstützenden SIP Leitung.

Network Connectivity

- › Bei einer ISDN-RAS Einwahl wird der Windows-Client schneller im Netzwerk registriert.
- › Die Paketlaufzeiten für Datenübertragungen mit kleinen Paketgrößen (z.B. VoIP) mittels IPsec-over-HTTPS wurden verbessert.
- › Bedingungen von Firewall-Regeln werden nun auch für Multicast-Pakete ausgewertet.
- › Wird ein RADIUS-Server über einen VPN-Tunnel angesprochen, wird die NAS-IP nun richtig übertragen.
- › Wird an das SYSLOG Modul ein %s übergeben (z.B. als Variable in einer URL), kommt es nicht mehr zu einem Geräteneustart.
- › Mit dem aktuellen Chrome Browser für Android-Geräte kann die LANCOM Konfiguration wieder über HTTPS erreicht werden.

LCOS Änderungen 8.82.0089 Rel

Korrekturen/Anpassungen

WLAN

- › Die Standard-Texte für das Public Spot Administrationsportal SmartTicket sind nun sprachenabhängig.
- › Der Default-Wert für das Protokoll der Public Spot Login-Seite wird auf HTTP gesetzt.
- › Im Public Spot Modul kann ein individuelles Fallback Template genutzt werden.
- › Die Standard Public Spot Login Seite kann über ein Textfeld personalisiert werden.
- › Weitere Optimierungen der Public Spot Templates
- › Für die Smartphone-/Tablet-Ansicht kann ein zweites Bild für die Anmeldemaske hochgeladen werden.

VoIP

- › Nachdem ein VoIP Telefonat beendet wurde, werden noch eingehende RTP-Pakete im SIP ALG nicht verworfen.
- › Der SIP ALG tauscht für Antwortpakete auf ein REGISTER die externe IP-Adresse durch die IP des internen Teilnehmers nun korrekt aus.

Network Connectivity

- › Der Netzwerktyp eines ARF-Netzwerks kann via CLI richtig gesetzt werden.
- › Der Wert „Destination-Cache-Limit“ der IPv6-Firewall kann via CLI gesetzt werden.
- › Ein Überlauf der Maskierungstabelle wird verhindert.
- › Wird eine PPTP-Verbindung z.B. durch einen Abbruch der Internetverbindung nur einseitig beendet, können auf einer neuen Verbindung auch dann weiter Daten übertragen werden, wenn das fehlgeschlagene Polling der alten Verbindung diese logisch abbaut.

LCOS Änderungen 8.82.0067 RC2

Korrekturen/Anpassungen

WLAN

- › Bucht man sich in ein LANCOM Public Spot Netzwerk ein, wird auf IOS-Geräten automatisch der Standard-Browser mit der Anmeldeseite geöffnet.
- › Die neue Public Spot Darstellung ist nun auch auf dem LANCOM L-321 verfügbar.
- › Der Titel der Webseite für ein fehlgeschlagenes SmartTicket Login wurde korrigiert.
- › Die SmartTicket Rufnummernübermittlung wurde in den neuen Templates berücksichtigt.

Network Connectivity

- Lehnt das LANCOM einen ISDN-Ruf für dyn. VPN ab, wird dies nicht als Fehler ausgegeben.
- VPN-Verbindungen mit einer Extranetadresse können auch dann wieder aufgebaut werden, wenn sie ohne Keepalive konfiguriert wurden.

LCOS Änderungen 8.82.0051 RC1

Neue Features

WLAN

- Für LANCOM-Router mit Public Spot-Option kann das Quell-VLAN bzw. die NAS-Port ID (Interface) des anfragenden WLAN-Clients in der URL übergeben werden.
- Eine dynamische VLAN Zuweisung für Public Spot Benutzer ermöglicht unterschiedliche Profileigenschaften (z.B. Bandbreite).
- Das Versenden von Multi- und Broadcasts kann für eine WLAN-Funkzelle deaktiviert werden.
- Unterstützung von 802.11u (Hotspot 2.0)
- Unterstützung einer Anmeldung eines Public Spot Benutzers ohne Browser (WISPr)
- Anhand der MAC-Adresse kann ein Public Spot Client zu einem späteren Zeitpunkt automatisch wieder angemeldet werden (ReLogin).
- Für die LANCOM 1781 Geräte kann die WLC-Option auf 12 Geräte erweitert werden.
- Ein Public Spot Benutzer kann automatisiert angelegt werden
- Verbesserte Darstellung der Public Spot Seiten auf Tablets und Smartphones.

Network Connectivity

- Anpassung des Syslog-Gültigkeit Wertebereichs
- Für den IPv6 DHCP-Server kann ein Reconfigure durchgeführt werden.
- Erweiterung der internen Syslog-Tabelle
- DNS ist pro ARF-Netzwerk konfigurierbar
- Die Firewall erkennt und unterbindet Quelladress-Flooding

Korrekturen/Anpassungen

WLAN

- Verwendet ein Benutzer mehrfach seinen PMS-Zugang (Property Management System), wird dies in der Accounting-Liste zusammengefasst.

Network Connectivity

- › Verbesserung der USB-Geräteerkennung nach einem Gerätereustart
- › Das LANCOM antwortet nicht mehr ungewollt auf ARP-Anfragen im LAN.
- › Nach einer USB Überstrombehandlung wird der USB-Port wieder aktiviert.

LCOS Änderungen 8.80.0159 RU1

Korrekturen/Anpassungen

Network Connectivity

- › Die Erkennung der Mobilfunkkarte beim Start des LANCOM wurde verbessert.

LCOS Änderungen 8.80.0157 RU1

Korrekturen/Anpassungen

WLAN

- › Die Konfiguration eines LANCOM 3850 ohne externe WLAN Karte lässt sich wieder fehlerfrei ins Gerät schreiben.
- › Die automatische Authentifizierung der MAC-Adresse im Public Spot Modul kann wieder genutzt werden.
- › Bei Verwendung des Public Spot SmartTicket funktioniert die URL-Weiterleitung nach dem Anmeldevorgang wieder.
- › Eine Funkfeldoptimierung beeinträchtigt nicht mehr die RADIUS-Konfiguration.

VoIP

- › SIP ALG kann auch bei LAN-LAN Routing verwendet werden.
- › SIP ALG verarbeitet auch mehrere Accounts eines Telekom Call&Surf IP Anschlusses.
- › SIP ALG berücksichtigt nun auch SIP Update-Requests.

Network Connectivity

- › Ein RADIUS-Server kann dem LANCOM wieder IPv4-Adressen zuweisen.
- › Verwendet man ein dynamisches IPv6 Präfix in Verbindung mit einer festen Adressvergabe, wird die zugewiesene Adresse wieder freigegeben, wenn das aktuelle Präfix abgekündigt wird.
- › Die Maskierungsadresse der WAN IP Liste wird nicht mehr zur Beantwortung von ARP Requests verwendet.
- › Dynamisches VPN über D-Kanal kann wieder genutzt werden.
- › Ein Eintrag in der DNS Weiterleitungstabelle wird auch ohne Neustart wirksam.
- › Sendet ein Server auf eine abgelaufene Session ein TCP ACK, wird dies vom LANCOM mit einem RST beantwortet.
- › Wurde der Internetgegenstelle kein DNS-Server zugewiesen, wird der DNS-Server unter TCP/IP->Adressen verwendet.

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.

Sichern der aktuellen Konfiguration

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

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf die alte Firmware **nicht mehr automatisch möglich**.

Wenn Sie Geräte, die Sie über eine Router-Verbindung oder WLAN-Punkt-zu-Punkt-Verbindung erreichen können, aktualisieren möchten, bedenken Sie bitte, dass Sie zuerst das entfernte LANCOM Gerät und anschließend das lokale LANCOM Gerät aktualisieren. Eine Anleitung zur Firmware-Aktualisierung erhalten Sie im LCOS-Referenzhandbuch.

Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umständen nicht mehr möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Um mehr Platz im Speicher zu schaffen, muss dann statt einer vollwertigen Firmware zunächst eine eingeschränkte, kleinere Firmware eingerichtet werden. Hierdurch steht für die andere Firmware im Gerät erheblich mehr Speicher zur Verfügung.

Diese Einrichtung ist nur einmalig erforderlich und wird mit einer „Minimalfirmware“ durchgeführt.

Nach dem Einspielen der Minimalfirmware steht die Firmsafe-Funktion des LANCOM nur noch in eingeschränktem Umfang zur Verfügung. Das Update auf eine neuere Firmware ist weiterhin problemlos möglich.

Das LANCOM Gerät arbeitet nach einem fehlgeschlagenen Update jedoch mit einer Minimalfirmware, die Ihnen ausschließlich den lokalen Zugriff auf das Gerät erlaubt. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.