Release Notes

LCOS
10.42 RU11

Inhaltsübersicht

03 **1. Einleitung**

03 **2. Das Release-Tag in der Software-Bezeichnung**

04 **3. Gerätespezifische Kompatibilität zu LCOS 10.42**

04 **4. Hinweise zu LCOS 10.42**
04 Informationen zu Werkseinstellungen

05 **5. Feature-Übersicht LCOS 10.42**

05 **5.1 Feature-Highlights 10.42**
05 Dynamic Path Selection

05 **5.2 Weitere Features LCOS 10.42**
05 Dynamic DNS Service für die Public Cloud
05 Cloud-managed Hotspot
06 BLE API für die Realisierung innovativer Location-based Services

07 **6. Historie LCOS 10.42**
07 LCOS-Änderungen 10.42.1113 RU11
08 LCOS-Änderungen 10.42.1037 SU10
09 LCOS-Änderungen 10.42.1036 RU9
15 LCOS-Änderungen 10.42.0890 RU8
16 LCOS-Änderungen 10.42.0889 RU7
19 LCOS-Änderungen 10.42.0740 RU6
21 LCOS-Änderungen 10.42.0612 RU5

22 LCOS-Änderungen 10.42.0611 RU4
26 LCOS-Änderungen 10.42.0473 RU3
28 LCOS-Änderungen 10.42.0383 RU2
30 LCOS-Änderungen 10.42.0280 RU1
31 LCOS-Änderungen 10.42.0277 Rel
34 LCOS-Änderungen 10.42.0212 RC3
36 LCOS-Änderungen 10.42.0155 RC2
38 LCOS-Änderungen 10.42.0037 RC1

39 **7. Allgemeine Hinweise**
39 Haftungsausschluss
39 Sichern der aktuellen Konfiguration
39 Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

1. Einleitung

Alle Mitglieder der LANCOM Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.42 RU11 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 7 „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. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen. Wird für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Dient zur nachträglichen Weiterentwicklung einer initialen Release-Version und enthält Detailverbesserungen, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard.

3. Gerätespezifische Kompatibilität zu LCOS 10.42

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 unterstütze LCOS-Version für Ihr Gerät finden Sie unter
https://www.lancom-systems.de/produkte/firmware/software-lifecycle-management/produkttabellen-lcos-lifecycle-management

4. Hinweise zu LCOS 10.42

Informationen zu Werkseinstellungen
Geräte, die mit LCOS 10.00 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 über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

5. Feature-Übersicht LCOS 10.42

5.1 Feature-Highlights 10.42

Dynamic Path Selection

Mit dem neuen Highlight-Feature Dynamic Path Selection routen Sie in Ihrem SD-WAN geschäftskritische Business-Anwendungen stets über die qualitativ beste Leitung. Das Feature überwacht dabei kontinuierlich Ihre WAN-Verbindungen in Bezug auf Last, Paketverlust, Latenz oder Jitter und entscheidet in Abhängigkeit der aktuellen Verbindungsqualität dynamisch über die optimale Leitung für bestimmte Anwendungen. Welche Leistungskriterien Sie für eine Anwendung an die WAN-Verbindung stellen, definieren Sie dabei flexibel selbst. Somit profitieren Sie in großen SD-WAN-Infrastrukturen mit mehreren WAN-Verbindungen im Active/Active-Modus von maximaler Performance und Ausfallsicherheit.

5.2 Weitere Features LCOS 10.42

Dynamic DNS Service für die Public Cloud

Die LANCOM Management Cloud (Public) wird zum DynDNS-Provider! Weisen Sie in den Standort-Einstellungen den dort eingesetzten Gateways einfach eine feste, selbstgewählte Sub-Domain zu (mycompany.dyndns-lmc.de). Diese Sub-Domain kann daraufhin beispielsweise in VPN-Gegenstellen wie dem LANCOM Advanced VPN Client hinterlegt werden. Somit bleiben mit der neuen LCOS 10.42 auch Gateways mit dynamischen WAN-IP-Adressen jederzeit über diesen Domain-Namen erreichbar.

Cloud-managed Hotspot

Erstellen Sie mit wenigen Klicks einen einfachen WLAN-Hotspot – direkt aus der LMC heraus. Ein zusätzliches Gateway oder ein WLAN-Controller mit LANCOM Public Spot Option sind hierfür nicht erforderlich. Über ein intuitiv zu bedienendes Menü individualisieren Sie Ihren Hotspot-Begrüßungsbildschirm mit Ihrem Logo sowie Ihren Unternehmensfarben und integrieren wichtige Informationen wie Impressum und Nutzungsrichtlinien für Ihre Hotspot-Benutzer. Anschließend weisen Sie das neue Hotspot-Netz den gewünschten Standorten zu und schon steht er Ihren Besuchern zur Verfügung.

BLE API für die Realisierung innovativer Location-based Services

Ob für die Innenraumlokalisierung von Patienten in Krankenhäusern, die Auswertung von Kundenaufkommen im Einzelhandel oder Asset Tracking im Logistik-Bereich: Für alle LANCOM Access Points mit Bluetooth Low Energy-Modul (BLE) steht nun eine neue API-Schnittstelle (REST) für die Einbindung ortsbezogener Dienste zur Verfügung. In Zusammenarbeit mit Drittanbietern ermöglicht diese die Realisierung einer Vielzahl ortsbezogener Dienste (Location-based Services, LBS) und innovativer IoT-Anwendungen.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 6 „Historie LCOS 10.42“.

6. Historie LCOS 10.42

LCOS-Änderungen 10.42.1113 RU11

Korrekturen / Anpassungen

Allgemein

→ Die OSPF-Interface-Kosten wurden aufgrund einer falschen internen Verarbeitung mit unkorrekten Werten dargestellt.

→ Das WWAN-Modul der LANCOM Router 1790VA-4G, 1790VA-4G+ und 1793VA-4G konnte sich im Zustand ‚deaktiviert' befinden. In der Folge konnten die Router keine mobile Internetverbindung aufbauen.

→ Wenn eine OSPF-Konfiguration gespeichert und in einem zweiten Schritt die Routen-Redistribution hinzugefügt wurde, kündigte sich der LANCOM Router nicht als ASBR (Autonomous System Boundary Router) an.

→ Wird die Feature-Aktivierung per Konsole initiiert und der Lizenz-Server ist nicht erreichbar, verbleibt die Aktivierung im Zustand ‚in process'. Wurde die Feature-Aktivierung anschließend erneut per Konsole initiiert, führte dies zu einem unvermittelten Neustart des Gerätes.

VoIP

→ Stellte der Voice Call Manager nach Auflösung des ‚SRV Resource Records' fest, dass dieser nicht mit dem SIP-Server mit der höchsten Priorität verbunden war, initiierte dieser einen Wechsel zu dem am höchsten priorisierten Server. Dazu sendete der Voice Call Manager ein Un-Register zu dem bisherigen SIP-Server, um die Verbindung zu diesem zu trennen. Wurde das Un-Register von dem bisherigen SIP-Server nicht beantwortet, wechselte der Voice Call Manager nicht zum korrekten SIP-Server.

→ Wenn ein vorgeschalteter Session Border Controller in der ‚o line' des ‚SDP-Offer' einen Wert nahe des erlaubten Maximums sendete, konnte es vorkommen, dass der Voice Call Manager in der ‚o line' des ‚SDP Answer' einen Wert versendete, welcher über dem erlaubten Maximum lag. Dies führte dazu, dass das Telefonat nicht zustande kam.

→ Wird ein Router mit Voice Call Manager vor einer SIP-TK-Ankage eingesetzt, fungiert dieser als Session Border Controller (SBC). Wenn in einem solchen Szenario ein eingehendes Telefonat eines Mobilfunk-Teilnehmers (VoLTE) direkt über die Funktion ‚Verbinden ohne Rückfrage' (Blind Call Transfer) weitergeleitet wurde, handelte der Voice Call Manager mit einer bestimmten Gegenstelle des SIP-Providers den Codec nicht korrekt aus. Dies führte dazu, dass das Telefonat abgebaut wurde.

LCOS-Änderungen 10.42.1037 SU10

Korrekturen / Anpassungen

Allgemein

→ Sicherheitsverbesserungen durch ein Update der OpenSSL-Version auf 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 und CVE-2022-4450).

LCOS-Änderungen 10.42.1036 RU9

Korrekturen / Anpassungen

Allgemein

→ Ein Router mit konfigurierter Verbindung zeigte im Backup-Zustand keine Maskierung der WAN-Gegenstelle an (prüfbar mit den Konsolenbefehlen ‚show ipv4-fib', ‚ls /status/ip-router/act.-ipv4-routing-table'). Hierbei handelte sich um einen Darstellungsfehler, da die Maskierung für die WAN-Gegenstelle aktiviert war.

→ Aufgrund eines DNS-Cache-Fehlverhaltens in der Zusammenarbeit mit dem LMC-Client konnte es vorkommen, dass ein per LMC verwalteter LANCOM Router nach dem Ausrollen und Aktivieren einer Konfiguration nach einiger Zeit einen unvermittelten Neustart ausführte.

→ Im Syslog von LANCOM Mobilfunk-Routern der 1900-Serie mit Dual-SIM wurde als Status für den SIM-Karten-Slot 2 immer der Status des Slot 1 verwendet.

→ Aufgrund einer Änderung im DHCPv6 bei DOCSIS-basierten Vodafone IPv6-Internetanschlüssen konnte es vorkommen, dass LANCOM Router nicht mehr an diesen Anschlüssen verwendet werden konnten.

→ Der HTTP-Client konnte keine URLs mit relativem Redirect verarbeiten. Dies führte dazu, dass es bei Verwendung einer URL mit relativem Redirect im ‚Automatic Firmware Updater' bei einem automatischen Firmware-Update zu einem unvermittelten Neustart des Gerätes kam.

→ Weder per Konsole, noch im LCOS-Menübaum konnte für den Parameter OCSP-AIA im Pfad ‚Setup/Certificates/SCEP-CA/Web-Interface/Profiles' das Zeichen ‚/' hinterlegt werden.

→ In einem Szenario aus Internet-Verbindung mit Backup und VPN-Verbindung mit Backup erfolgte nach einem Ausfall der Internet-Verbindung ein Rückfall auf die Backup-Verbindung. Dadurch wurde auch der Aufbau des VPN-Backups initiiert. In Einzelfällen konnte es vorkommen, dass die Haupt-VPN-Verbindung vor dem VPN-Backup aufgebaut wurde. In diesem Fall wurde angezeigt, dass das VPN-Backup noch aktiv war (‚Status/WAN/Backup' auf ‚Yes').

→ Im Syslog wurden wiederholt der Mobilfunk-Providername und die Cell-ID / Location Area Codes ausgegeben, obwohl diese nur bei einer Änderung der Daten ausgegeben werden sollten.

→ Erfolgte in einem VRRP-Stenario ein Wechsel der Schnittstelle zum BGP Peer (etwa durch Wechsel der Internet-Verbindung), verblieb die BGP-Verbindung anschließend im Status ‚idle' und wurde nicht wieder aufgebaut.
→ Bei einer Zertifikats-Aktualisierung überprüft die CA des Antragstellers das Zertifikat gegen die CRL. OpenSSL war aber so konfiguriert, dass diese Prüfung nur bei einer Root-CA möglich war. Dies führte dazu, dass die Aktualisierung einer Sub-CA per SCEP fehlschlug.
→ Obwohl der Config Sync-Dienst zum WAN in der Konfiguration eines LANCOM Routers deaktiviert war (Standard-Einstellung), wurde der Dienst in der LMC als aktiviert und mit dem Sicherheits-Status ‚kritisch' angezeigt.
→ Eine im Rollout-Wizard angegebene URL für ein Popup wurde falsch behandelt. Es wurden nicht nur die URL-Parameter passend enkodiert, sondern auch die Teile des Pfades zuvor.
→ Wenn der DHCPv6-Client auf ein ‚DHCP renew' eine Antwort mit mehreren gleichen DHCP-Optionen vom DHCPv6-Server erhielt (laut RFC 8415 verboten), verwarf der DHCPv6-Client das Antwort-Paket. Dies führte dazu, dass die IPv6-Adresse nicht erneuert wurde und bis nach der erneuten DHCPv6-Aushandlung keine Kommunikation mehr über diese Schnittstelle möglich war.
Der DHCPv6-Client verwendet jetzt immer die erste DHCP-Option und ignoriert die restlichen Optionen.
→ In einem TACACS+-Szenario wurde bei einer Änderung des Hauptgeräte-Passwortes über die Kommandozeile der zusätzliche Parameter ‚-n' nicht erkannt.

VPN

→ Wenn eine Konfiguration als Skript in einen LANCOM Router geladen wurde (*.lcs-Datei) und diese keine Unterschiede in der Konfiguration von eingerichteten VPN-Client-Verbindungen aufwies, wurden bestehende VPN-Client-Verbindungen trotzdem getrennt.
→ In seltenen Fällen konnnte es vorkommen, dass bei aktiver Backup-Internetverbindung über das WWAN das Routing vom LAN ins VPN nicht mehr funktionierte.

WLAN

→ Ein logisches WLAN-Netzwerk in einem WLC-Szenario wurde nach dem Entfernen aus der Konfiguration des WLC weiterhin im LANmonitor angezeigt.

VoIP

→ In einem Szenario mit einer Swyx-TK-Anlage und einem CTI+-Teilnehmer versendete der Voice Call Manager bei einer Weiterleitung des Telefonats an einen Mobilfunk-Teilnehmer (VoLTE) ein Re-INVITE an den CTI+-Teilnehmer. Im anschließenden „SIP 200 OK“ des CTI+-Teilnehmers war ein neuer ‚Record Route‘ Header enthalten, den der Voice Call Manager im nachfolgenden „ACK“ übernahm, statt den bisherigen Header zu übernehmen. Dies führte dazu, dass das Telefonat durch den SIP-Provider abgebaut wurde.

→ Wenn der Router in einem Szenario mit angebundener SIP-TK-Anlage als SBC fungierte und einen eingehenden Anruf erhielt, bei dem nach 15 Minuten (Session-Expires: 1800) sowohl von der SIP-TK-Anlage als auch vom Provider ein Update mit einem Refresh gesendet wurde, verwendete der Router im vom Provider erhaltenen „200 OK“ bei der Weiterleitung an die SIP-TK-Anlage im Via-Header eine neue Branch-ID. Diese war der SIP-TK-Anlage nicht bekannt und wurde somit verworfen. Dies führte dazu, dass das Telefonat nach 15 Minuten durch die SIP-TK-Anlage beendet wurde.
Weiterhin verwendete der Router im Route Header und im Request Uri die Informationen aus dem letzten UPDATE-Paket statt aus dem INVITE (separater Anruf). Dies führte dazu, dass das Telefonat nach 45 Minuten vom Provider mit der Meldung „481 Call Leg/Transaction Does Not Exist“ abgebrochen wurde.

→ Bei ausgehenden Anrufen konnte es vorkommen, dass der LANCOM Voice Call Manager im SDP eine DTMF-Codec-Ordnungsnummer doppelt verwendete, was dazu führte, dass der Anruf seitens des Providers mit der Meldung „488 SDP Parameter Error In SIP Request“ abgelehnt wurde und nicht zustande kam.

→ Bei einem Wechsel auf einen anderen SIP-Server (initiiert durch eine eDNS-Nachricht) sendete der Router das ‚Deregister‘ an den neuen SIP-Server statt an den alten. Ein ‚Deregister‘ wird jetzt an den alten SIP-Server geschickt, wenn sich die Priorität der Server geändert hat oder ein Wechsel auf den höchstpriorisierten Server erfolgt.

→ Wird bei einem eingehenden Telefonat vom SIP-Provider (z.B. Deutsche Glasfaser) im INVITE neben dem ‚Session-Expires Header' (Ablaufwert für die Session, z.B. 1860 Sekunden) zusätzlich der Parameter ‚refresher=uas' (UAS = User Agent Server) übermittelt, erwartet der SIP-Provider vom Router einen Session-Refresh nach der Hälfte des Wertes im ‚Session-Expires Header' (in diesem Beispiel also 930 Sekunden). Dazu wird auf dem Router ein ‚Session Refresh Timer' mit einer entsprechenden ‚Expiration Time' gestartet. Wenn der SIP-Provider kurz vor Ablauf des ‚Session Refresh Timers' auf dem Router ein Re-INVITE mit einem ‚Session-Expires Header' (z.B. erneut 1860 Sekunden) und dem Parameter ‚refresher=uas' an den Router sendete, startete der Router den ‚Session Refresh Timer' neu, statt den vorhandenen Timer ablaufen zu lassen und die Session mit dem SIP-Provider zu erneuern. Dies führte dazu, dass das Telefonat nach Ablauf der ursprünglichen ‚Expiration Time' vom SIP-Provider abgebaut wurde.
Ein ‚Session Refresh Timer' wird jetzt nicht mehr neu gestartet, sofern dieser bereits aktiv ist, es sei denn, die neue ‚Expiration Time' ist kleiner als der verbleibende Wert des Timers. In diesem Fall wird der neue Wert übernommen.

→ Der Voice Call Manager überprüft bei einem ausgehenden Telefonat, ob der SIP-Benutzer lokal vorhanden ist. Dabei wurden im SIP-Header die Felder PAI, PPI und FROM in der angegebenen Reihenfolge durchlaufen, aber lediglich das erste Feld mit einer Rufnummer überprüft. War in dem Feld für die PAI oder die PPI zwar eine Nummer vorhanden, stimmte aber nicht mit dem konfigurierten SIP-Benutzer überein, so konnte der SIP-Benutzer keine ausgehendenden Telefonate initiieren.
Die Felder werden jetzt alle der Reihe nach geprüft, sofern diese eine Rufnummer enthalten und der Benutzer noch nicht verifiziert wurde.

→ Bei Verwendung einer SIP-PBX-Leitung kam es bei eingehenden Telefonaten an einen in einem Rufnummernblock enthaltenen Teilnehmer (zusammengefasst in einer Call Route mit der Wildcard #) zu einem signifikant längeren Rufaufbau, wenn der angerufene Teilnehmer lediglich eine Ziffer hatte (die Wildcard #), da in diesem Fall das ‚Overlap Dialing' durchlaufen wurde.

→ Der Voice Call Manager überprüfte seinen DNS-Cache alle 5 Sekunden auf abgelaufene SRV-Records (TTL=0) und löschte diese anschließend. Traf die Antwort auf eine DNS-Anfrage erst nach Löschung des entsprechenden SRV-Records am Voice Call Manager ein, wurde die SIP-Leitung abgebaut und im Syslog die Meldung „generic failure“ ausgegeben.
Abgelaufene SRV-Records werden jetzt erst nach zweimaliger Überprüfung (insgesamt 10 Sekunden) aus dem DNS-Cache entfernt. Weiterhin wird die SIP-Leitung nicht abgebaut, solange die vorhandene Verbindung zum SIP-Server funktioniert.

→ Bei der Verwendung von CTI+ an einer Netphone-TK-Anlage konnte es in Verbindung mit dem LANCOM VoIP-Router zu einseitiger Sprachübertragung kommen, da die lokal erzeugten RTP-Header nicht mit den durchgereichten RTP-Headern synchronisiert waren.

→ Wenn ein Benutzer, der hinter einer Octopus Netphone-TK-Anlage angeschlossen war, eine vSDP-Nummer anrief, bei welcher eine Rufweiterleitung auf ein VoLTE-Mobiltelefon mit Soundlogo eingerichtet war, war beim Anrufer lediglich der ‚Caller Ringback Tone (RBT)‘ zu hören und nicht das Soundlogo.

→ Beim Registrieren einer SIP-Leitung konnte die DNS-Ausflösung mit der höchsten DNS-Prioritätsstufe ‚P-CFCS‘ nicht durchgeführt werden.

→ Wenn der Voice Call Manager bei einem ausgehenden Telefonat ein ‚Session Progress‘ Paket mit dem Tag ‚inactive‘ im ‚P-Early-Media Header‘ empfing, wurden die RTP-Streams beendet und nicht wieder neugestartet. Dadurch war keine Sprach-Kommunikation möglich.

→ Wurde in einem Szenario mit angebundener SIP-TK-Anlage bei einem ausgehenden Telefonat während der ‚Early Media Phase‘ ein ‚UPDATE request‘ vom SIP-Provider empfangen, leitete der Voice Call Manager dieses an die angeschlossene SIP-TK-Anlage weiter, obwohl dies zu diesem Zeitpunkt nicht möglich war. Die SIP-TK-Anlage quittierte dies mit der Fehlermeldung „500 Internal Server Error“. Dadurch konnten keine RTP-Daten übertragen werden und es war keine Sprach-Kommunikation möglich.
In einem solchen Fall beantwortet der Voice Call Manager das ‚UPDATE request‘ jetzt mit einem „200 OK“ und sendet die SDP-Informationen in einem ‚Reliable Provisional Response‘.

→ Empfing der Voice Call Manager in einem Szenario mit CompanyFlex-Anschluss von einem ISDN-Benutzer ein SETUP für eine interne Anruf-Weiterschaltung (AWS) mit einer zweiten Rufnummer im Feld ‚Calling Party Number', welche sich nicht im lokalen Rufnummern-Kreis befand, sendete der Voice Call Manager anschließend ein INVITE mit der zweiten Rufnummer als PPI an den Provider. Dies wurde vom Provider mit der Fehlermeldung „403 Forbidden" abgelehnt.

LCOS-Änderungen 10.42.0890 RU8

Neue Features

→ Unterstützung für neue Temperatur-Sensor-Hardware bei den LANCOM Geräten

- 1640E
- 1790EF
- 1790VA
- 1790VA-4G+
- 1790VAW

LCOS-Änderungen 10.42.0889 RU7

Korrekturen / Anpassungen

Allgemein

→ Es wurde eine Schwachstelle in der OpenSSL-Bibliothek behoben (CVE-2022-0778).

→ Es wurde eine Schwachstelle in der zlib-Bibliothek behoben (CVE-2018-25032).

→ Wenn bei einem LANCOM Mobilfunk-Router mit eingerichteter Mobilfunk-Backup-Verbindung keine SIM-Karte eingesteckt war und auf die Backup-Verbindung geschaltet wurde, führte dies zu immer wiederkehrenden Neustarts des Mobilfunk-Moduls. Dies konnte vereinzelt auch zu unvermittelten Neustarts des Gerätes aufgrund von Speicherverlusten führen.

→ Lokale Interfaces konnten über einen SNMP-Walk auf die ipAddrTable (.1.3.6.1.2.1.4.20) nicht ausgelesen werden. Stattdessen wurden nur Informationen zu den WAN-Interfaces ausgegeben.

→ In der Tabelle ‚/Status/Routing/BGP/Messages' waren ab einer unterschiedlichen Zahl von Einträgen unleserliche Einträge vorhanden, welche durch eine fehlerhafte Angabe der Tabellengröße hervorgerufen wurden.

→ Nach einer Reinitialisierung des WWAN-Modems beim LANCOM 1790VA-4G+ mit dem Befehl ‚do /status/usb/reinit' war das Modem ohne Funktion. Nur mit einem kompletten Neustart des Routers konnte die Funktionalität des WWAN-Modems wieder hergestellt werden.

→ Da die SNMP EngineID bei LANCOM Geräten im Enterprise-ID-Format ausgelesen wird, war diese bei einer Abfrage über eine OID um 1 Byte zu kurz, weshalb zwei Zeichen fehlten. In der Folge meldeten die Geräte, dass sie die gleiche SNMP EngineID verwenden.

→ Wenn ein NTP-Netzwerk für den NTP-Server per Konsole eingetragen wurde, fand dieses keine Anwendung. Dies führte dazu, dass Geräte in diesem Netzwerk keine Zeit von diesem NTP-Server beziehen konnten. Im NTP-Trace wurde die Fehlermeldung „LAN-Request received, but sender is not in Networklist" ausgegeben.

→ Wenn ein Access Point oder Router mit mindestens zwei Netzwerken verwendet und die IP-Adresse in diesen Netzwerken per DHCP bezogen wurde, konnte es vorkommen, dass der HTTP-Client für den Verbindungsaufbau zur LMC statt der LMC Loopback-Adresse die undefinierte IP-Adresse 0.0.0.0 verwendete. Dies führte dazu, dass für die Verbindung zur LMC eine IP-Adresse aus einem anderen Netzwerk verwendet wurde und die Verbindung zur LMC immer wieder abbrach.

→ In LCOS 10.42 wurde die Mobilfunk-Verbindungshistorie im Pfad ‚/Status/Modem-Mobile/History' von 100 auf 512 Einträge erweitert. Nach einem Firmware-Update auf eine entsprechende Version wurde die Tabelle nicht korrekt auf die neue Größe konvertiert und daher weiterhin eine Tabelle mit 100 Einträgen verwendet. Wenn mehr als 100 Einträge geschrieben wurden, führte dies zu einem unvermittelten Neustart des Routers.

→ Das WEBconfig- bzw. TLS-Geräte-Zertifikat eines mit LCOS betriebenen LANCOM Gerätes wurde über das Ablaufdatum im Jahr 2024 hinaus nicht automatisch vom Gerät verlängert.

→ Es konnte beim Versenden einer E-Mail durch den Router zu einem unvermittelten Neustart kommen.

→ Bei der Nutzung von OSCP wurde ein abgelaufenes Zertifikat weiterhin verwendet, auch wenn dieses bereits per SCEP erneuert wurde.

→ Wenn als Antwort auf einen gesendeten TXT-Record ein leerer TXT-Record empfangen wurde, konnte der DNS-Server im LANCOM Router diese Antwort nicht verarbeiten. In der Folge verwarf dieser die Antwort.

→ Beim LANCOM 1790VA-4G+ wurden Informationen zum verwendeten Mobilfunk-Band nicht im Status angezeigt.

→ In einem VRRP-Szenario mit einzelnen WAN-Gegenstellen, in welchem diese Gegenstellen zusätzlich zu einem Loadbalancer zusammengefasst wurden, konnte es vorkommen, dass der VRRP-Slave im Sekundentakt versuchte, die WAN-Gegenstellen aufzubauen.
In der Folge stieg die CPU-Last des Gerätes und es trat ein Speichermangel auf. Es wurde nun eine Pause zwischen den einzelnen Verbindungsversuchen programmiert, wodurch das Gerät nicht mehr an seine Leistungsgrenze gebracht wird.

WLAN

→ Bei Verwendung eines WLC-Tunnels müssen Datenpakete eine Paketgröße mit einem Vielfachen von 8 aufweisen. Je nach verwendeter PMTU konnte es aber vorkommen, dass der WLAN-Controller Datenpakete mit einer Paketgröße sendete, bei denen dies nicht der Fall war. Dies führte in Verbindung mit Access Points mit LCOS LX-Betriebssystem dazu, dass diese die entsprechenden Datenpakete nicht verarbeiten konnten und die Pakete somit verworfen wurden.

→ Wenn in der Konfiguration eines LANCOM WLAN-Controllers im Menü ‚WLAN-Controller → AP-Konfiguration → IP-Parameter-Profile' nur die Netzmaske eines IP-Profils verändert wurde, übertrug der WLC diese Änderung zwar an verwaltete Access Points, die IP-Konfiguration der Access Points blieb jedoch unverändert.

→ Per WEBconfig konnte in der LEPS-Konfiguration kein WLAN-Client ohne Angabe einer Passphrase hinzugefügt werden, obwohl die Angabe einer Passphrase optional angegeben war.
→ Bei Verwendung der LAN-Bridge auf einem Access Point oder WLAN-Router (Standard-Einstellung) wurde bei DHCP-Requests immer die MAC-Adresse des LAN-Interfaces eingesetzt. Dies führte dazu, dass per WLAN-Punkt-zu-Punkt-Verbindung oder per AutoWDS angebundene Access Points oder WLAN-Router das DHCP-Offer verwarfen und somit keine IP-Adresse beziehen konnten.
→ Das Zeichen ‚ALT+34' konnte bei der Vergabe eines WPA-PSK nicht verwendet werden.

VoIP

→ Bei einem ‚Vodafone Anlagenanschluss Plus' konnte es bei eingehenden Anrufen vorkommen, dass die ‚Halten'-Funktion nicht ausgeführt werden konnte, da im RE-INVITE des Voice Call Managers keine P-Preferred-Identity (PPI) enthalten war.
→ Es konnte beim Versand eines SNMP-Traps mit Informationen zu ISDN-Benutzern zu einem unvermittelten Neustart des Routers kommen.
→ In einem Szenario, in welchem eine Panasonic SIP-TK-Anlage (SIP-TK KX-NCP500) an einem LANCOM Router angeschlossen war, konnte eine Anrufweiterleitung aufgrund einer fehlerhaften SDP-Kommunikation seitens der TK-Anlage scheitern. Im LCOS wurde nun ein Workaround eingebaut, welcher den Fehler abfängt und eine Kommunikation ermöglicht.
→ Wenn ein ausgehender Anruf vom angerufenen Teilnehmer an einen dritten Teilnehmer weitergeleitet wurde und der dritte Teilnehmer ein DTMF-Menü zur Anrufbearbeitung anbot, funktionierte die DTMF-Kommunikation über Tastentöne nicht mehr. In der Folge konnte das vom dritten Teilnehmer angebotene DTMF-Menü nicht bedient werden.

LCOS-Änderungen 10.42.0740 RU6

Korrekturen / Anpassungen

Allgemein

→ In einer BGP-Community konnte der Wert „0“ nicht verwendet werden.

→ Erfolgreiche Admin-Logins ins WEBconfig wurden zwar in der Login-Tabelle erfasst, der Zähler für die Logins blieb jedoch unverändert.

→ Wurde eine Firewall-Regel mit ‚bedingter Übertragung‘ durchlaufen und es traf keine Bedingung in einer weiteren Firewall-Regel zu, wurde das Paket im IP-Router mit der Fehlermeldung „Network unreachable (no route) ⇒ Discard“ verworfen, statt das Paket nachträglich per „ACCEPT“ zu erlauben.

→ In privaten LMC-Installationen funktionierte der WEBconfig-Fernzugriff über den Webbrowser nicht, wenn zu viele HTTP-Cookies verwendet wurden.

→ Ein externes Modem, welches an einem LANCOM Router angeschlossen war und eine sog. APIPA-Adresse (Automatic Private IP Addressing) besaß, konnte vom LANCOM Router nicht erreicht werden, da diese Adressen beim Proxy-ARP aus dem LAN nicht zugelassen waren.

→ Wenn in der Tabelle der Zugriffsstationen eine IP-Adresse eingetragen war, konnte aus der LANCOM Management Cloud (LMC) heraus keine WEBconfig-Session zu einem Gerät aufgebaut werden.

→ Wenn ein Portforwarding mit einem Port zwischen 16384 und 65535 eingerichtet wurde, konnte es vorkommen, dass dieser Port auch für eine dynamische Port-Aushandlung eines weiteren Netzwerk-Teilnehmers verwendet wurde. In diesem Fall wurden die eingehenden Pakete an das Ziel der dynamischen Port-Aushandlung statt an das eigentliche Ziel weitergeleitet.

→ Im WEBconfig (z.B. im Menü ‚Konfiguration / IP-Router / Routing / IPv6-Routing-Tabelle‘) wurde ein IPv6-Präfix aufgrund einer fehlerhaften HTML-Kodierung falsch dargestellt.

→ Aufgrund einer fehlerhaften Sortierung der Port-Forwarding-Tabelle konnte es bei sich überlappenden Einträgen (mit unterschiedlichen Protokollen) vorkommen, dass das Port-Forwarding nicht korrekt funktionierte.

→ In einem VRRP-Szenario mit einzelnen WAN-Gegenstellen, in welchem diese Gegenstellen zusätzlich zu einem Loadbalancer zusammengefasst wurden, konnte es vorkommen, dass der VRRP-Slave im Sekundentakt versuchte, die WAN-Gegenstellen aufzubauen.
In der Folge stieg die CPU-Last des Gerätes und es trat ein Speichermangel auf. Es wurde nun eine Pause zwischen den einzelnen Verbindungsversuchen programmiert, wodurch das Gerät nicht mehr an seine Leistungsgrenze gebracht wird.

WLAN

→ Es konnte in einem WLC-Cluster-Szenario vorkommen, dass die Sub-CA auf dem Slave ablief und kein neues Zertifikat bezogen wurde. Dies führte dazu, dass die auf dem Slave angemeldeten Access Points nicht verwaltet werden konnten.

→ Es konnte vorkommen, dass im WEBconfig-Menü ‚Public Spot Benuter verwalten' keine Ausdrucke von angelegten Public Spot-Benutzerdaten erstellt werden konnten.

LCOS-Änderungen 10.42.0612 RU5

Korrekturen / Anpassungen

Allgemein

→ Ein Script-Upload per HTTPS führt nicht mehr zum Watchdog.

LCOS-Änderungen 10.42.0611 RU4

Korrekturen / Anpassungen

Allgemein

→ Ein Zugriff per LL2M auf ein Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „user unknown on remote system“ quittiert.

→ Bei Verwendung von Zertifikaten mit Elliptic Curve Algorithmus für RADSEC konnte die TLS-Aushandlung nicht erfolgreich abgeschlossen werden. Weiterhin konnte der Private Key eines Zertifikats mit Elliptic Curve-Algorithmus nicht in den RADSEC-Slot hochgeladen werden. Der Import-Vorgang wurde mit der Meldung „FAILURE“ abgebrochen.

→ Das Erstellen eines Wireshark-Trace per LCOSCap auf einem Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „cannot retrieve PSK“ quittiert.

→ Die ‚Dynamic Path Selection‘ konnte die DNS-Auflösung nicht über eine Loopback-Adresse durchführen. Wenn ein DNS-Server nur über eine Loopback-Adresse mit einem von 0 abweichenden Routing-Tag angesprochen werden konnte, führte dies dazu, dass die DNS-Auflösung des Messziels (z.B. measurement1.cloud.lancom.eu) nicht möglich war. Dadurch wurden in dem DPS-Graphen in der LMC unvollständige Daten angezeigt.

→ Mit dem Konsolenbefehl ‚passwd -n‘ kann eine Passwortänderung ohne Abfrage durchgeführt werden. Dabei wurde die Änderung nicht für den SNMP-Zugriff übernommen, sodass ein SNMP-Zugriff mit dem alten Passwort möglich war.

→ Beim Anlegen eines RADIUS-Benutzers via WEBconfig konnte das Benutzerprofil nicht gespeichert werden, wenn dort keine Passphrase eingetragen wurde.

→ Der Rollout-Wizard wurde bei einem vorhandenen Rollout-Benutzer nicht automatisch gestartet, sondern man musste sich explizit als Rollout-Benutzer am System anmelden, damit der Wizard startete.

→ Nach einer Aktualisierung auf LCOS 10.42 RU3 konnte es vorkommen, dass nach einer Konfigurations-Synchronisierung mit der LANCOM Management Cloud (LMC) eine Firewall-Regel, welche ein DNS-Ziel enthielt, nicht mehr mit LANconfig editiert werden konnte.

→ Bei Verwendung des Stationsobjektes LOCALNET in Firewall-Regeln wurden per RIP und BGP gelernte Routen dem LOCALNET zugeordnet. Dies konnte dazu führen, dass die CPU des Routers aufgrund sehr vieler Filter-Regeln eine hohe Auslastung aufwies.
Dem Stationsobjekt LOCALNET werden jetzt nur noch Netzwerke im Status ‚Connected LAN‘ zugeordnet.

→ Das Ausführen eines LCOS-Skriptes bei Nutzung der automatische Netzwerkauswahl führte bei LANCOM Geräten mit 4G-Modul dazu, dass eine bestehende WWAN-Verbindung abgebaut wurde, auch wenn es keine Konfigurations-Änderung an der WWAN-Verbindung gab, die einen Neustart der Verbindung nötig machte.
→ Wenn ein LANCOM Router oder Access Point einem ARF-Netzwerk angehörte, welches ein Routing-Tag ungleich 0 besaß, wurde als LLDP-Information nicht die IP-Adresse des Gerätes sondern dessen MAC-Adresse angezeigt.
→ Durch ein Fehlverhalten im DHCP-Relay-Agent eines LANCOM Routers konnte es vorkommen, dass ein Netzwerk-Client keine IP-Adresse beziehen konnte, wenn der LANCOM Router als DHCP-Relay konfiguriert war.
→ Bei Verwendung von TACACS+ konnte die Konfiguration nicht von einem TACACS+-Benutzer per LANconfig gespeichert werden, wenn das Hauptgeräte-Passwort als verschlüsselter Hashwert vorlag.
→ Wenn eines der Standard-Netzwerke INTRANET oder DMZ nicht verwendet wurde (IP-Adresse 0.0.0.0) und als ‚Netzwerktyp' die Option ‚Intranet' ausgewählt war, wurde dieses Netzwerk vom Router als aktiv behandelt. Wurde einem selbst angelegten Netzwerk das gleiche Interface wie das Standard-Netzwerk zugewiesen (z.B. LAN-1), war keine Kommunikation möglich, da die Pakete von der Firewall mit der Fehlermeldung „Filter info: packet received from invalid interface LAN-1" verworfen wurden.

WLAN

→ In LCOS 10.42 wurde der Übertragungskanal zwischen Access Point und ePaper Display nicht korrekt an den ePaper Server übertragen, was dazu führte, dass ePaper Displays als „Nicht erreichbar" angezeigt wurden und keine Kommunikation zwischen Server und Display stattfinden konnte.
→ In LCOS 10.42 konnte sich das ePaper-Modul des Access Points aufgrund eines fehlenden ‚restart'-Befehls in der Firmware nicht automatisch beim ePaper Server melden. In der Folge verlor der Access Point die Verbindung zum ePaper Server. Nach einem Neustart des Access Points wurde dieser zwar wieder mit dem ePaper Server verbunden, verlor aber die Verbindung später erneut.
→ Wenn man im WEBconfig-Menü ‚Setup-Wizards / Public-Spot-Benutzer einrichten' mehr als einen Voucher gleichzeitig erstellt hatte, wurde zum Ende des Erstellvorgangs das Fenster zum Drucken aller erstellten Voucher nicht angezeigt.
→ In LCOS 10.40 oder höher konnte es vorkommen, dass die zertifikatsbasierte RADIUS-Authentifizierung mit ECDSA-Zertifikaten fehlschlug. Die ECDSA-Signaturen wurden jetzt korrigiert.

→ Bei Verwendung des Client-Management im WLAN konnte es sporadisch zu einem unvermittelten Neustart kommen, wenn der Environment Scan durchgeführt wurde.
→ Bei Access Points und WLAN-Routern mit IEEE 802.11ac WLAN-Modul wurde bei fester Einstellung der RX/TX-Übertragungsraten im WLAN auf einen Wert größer als 6 MBit/s die Basisdatenrate (Management Frames) weiterhin mit 6 MBit/s übertragen.

VPN

→ Während der Aushandlung einer IKEv2-Verbindung sendete der aufbauende Router (VPN-Initiator) immer den Parameter ‚MANAGEMENT_IP4_ADDRESS' des Features ‚Dynamic Path Selection' mit, auch wenn dies nicht aktiv war. Wenn dieses Feature vom annehmenden Router (VPN-Responder) nicht unterstützt wurde, konnte dies dazu führen, dass die VPN-Verbindung nicht aufgebaut werden konnte.

VoIP

→ Sendete ein VoIP-Client bei einem ausgehenden Anruf den Parameter ‚rtcp-rsize' mit, erkannte der LANCOM Router diesen Parameter als ‚Invalid' und lehnte das ‚Invite' mit der Meldung „406 SDP - not acceptable" ab. In der Folge kam der ausgehende Ruf nicht zustande.
→ Bei einem eingehenden ISDN-Anruf konnte es vorkommen, dass der externe Anrufer den Angerufenen nicht hören konnte (einseitige Sprachübertragung), da das ‚Media Attribute (a): nortpproxy:yes' die Übermittlung von RTP-Daten verhinderte.
→ Eine Weiterleitung eines eingehenden externen Telefonates von einem SIP-Teilnehmer an einen Analog-Teilnehmer führte zu einem unvermittelten Neustart des Routers.
→ Es konnte vorkommen, dass Telefonate über den SIP-ALG nicht übertragen wurden, da der externe Port vom Router als ungültig deklariert wurde. Die Pakete wurden dann mit der Fehlermeldung „ICMP Destination unreachable (Port unreachable)" abgelehnt.
Weiterhin funktionierte die Bandbreiten-Reservierung im SIP-ALG nicht mehr.
→ Die Funktionen ‚Rückfrage' und ‚Vermitteln' funktionierten nicht, da der Router im „200 OK" nach dem Re-INVITE keine SDP-Informationen mitsendete.

→ In einem Szenario mit einer Swyx Mediabridge erfolgt nach Rufaufbau ein REFER mit dem eigentlichen Ziel des Telefonates im ‚Refer-To'-Header. Daraufhin sendet der Router ein INVITE zu diesem ‚Refer-To'-Ziel über die Swyx TK-Anlage. Im Fehlerfall antwortete die Swyx TK-Anlage nicht mit einem „200 OK", sondern mit der Fehlermeldung „500 Server Internal Error". Der Router versuchte in diesem Fall das INVITE auf einer anderen Leitung zu senden. Da hierfür aber noch die Replace-Informationen aus dem REFER verwendet wurden, sendete der Router das INVITE erneut über die Gateway-Leitung an die Swyx TK-Anlage.
Ein INVITE wird jetzt nicht mehr auf einer Gateway-Leitung versendet, nachdem auf dieser die Fehlermeldung „500 Server Internal Error" empfangen wurde. Weiterhin wartet der Router auf ein „BYE" der Swyx TK-Anlage und beendet anschließend den Rufaufbau. Wenn kein „BYE" von der Swyx TK-Anlage empfangen wird, sendet der Router das „BYE" und beendet den Rufaufbau.

LCOS-Änderungen 10.42.0473 RU3

Korrekturen / Anpassungen

Allgemein

→ Wenn H.323 in der Konfiguration aktiviert ist (Standardeinstellung), wird dieses nach einer Aktualisierung auf LCOS 10.42 RU3 deaktiviert. Wird das Protokoll in der Konfiguration wieder aktiviert, wird eine Syslog-Nachricht generiert.

→ Das Mobilfunk-Modem sendete im IPv6-Betrieb keine regelmäßigen Router Advertisements (RA). Dies führte dazu, dass nach Ablauf der Router Lifetime von 65.535 Sekunden (ca. 18 Stunden) der Router kein Gateway mehr hatte und somit keine IPv6-Kommunikation mehr möglich war.
Kurz vor Ablauf der RA Lifetime wird jetzt eine Router Solicitation (RS) zwecks Update der Router Lifetime versendet.

→ Wurde ein Router oder Access Point als DHCP-Client verwendet und auf diesem ein statischer Routing-Eintrag mit einem Gateway (Next Hop) erstellt, so wurde das per DHCP gelernte Gateway nicht korrekt übernommen. Dies führte dazu, dass keine Kommunikation über die statische Route möglich war.

→ Bei Verwendung bestimmter DSLAMs auf der Providerseite konnte es mit einem LANCOM 1926VAG aufgrund einer Inkompatibilität zwischen dem verbauten DSL-Modem und dem DSLAM vorkommen, dass der DSLAM nicht alle erforderlichen Parameter an das DSL-Modem übermittelte. Dies führte dazu, dass kein DSL-Sync zustande kam und somit auch keine DSL-Verbindung aufgebaut werden konnte.

→ Die Wireless ePaper-Features ‚SyncProfile' und ‚Label Events' waren nicht funktionsfähig.

→ Eine deaktivierte IPv4-Firewall-Regel, in welcher einer oder mehrere Port-Bereiche angegeben waren, wurde beim Zurückschreiben der Konfiguration falsch interpretiert, was dazu führte, dass die Konfiguration nicht in den LANCOM Router zurückgeschrieben werden konnte.

VPN

→ Versuchte der Router während eines VPN-Verbindungsaufbaus im Zeitfenster zwischen IKE-Aushandlung und dem Wechsel in den Status ‚Up' ein Paket über die VPN-Verbindung zu senden, wurden alle Pakete verworfen.

→ Wurde bei aktivem Port-Forwarding für den UDP-Port 500 eine VPN-Verbindung von einem nachgelagerten Router initiiert, wurden die Antwort-Pakete durch das Port-Forwarding nicht in der IPSec-Maskierungs-Tabelle eingetragen. Dies führte dazu, dass die VPN-Verbindung nicht funktionierte.

WLAN

→ Der Public Spot ‚Idle-Timeout' konnte nicht über die XML-Schnittstelle gesetzt werden. Der im XML-Befehl gewählte Wert wurde dabei nicht übernommen und stattdessen der im Gerät eingetragene Wert ausgegeben.

VoIP

→ In Einzelfällen kann es vorkommen, dass bei einem eingehenden Telefonat während der Early-Media-Phase ein UPDATE vom Anrufer anstatt vom Angerufenen gesendet wird. In einem solchen Fall wurde das UPDATE vom Router wieder auf die SIP-Leitung gesendet anstatt an den lokalen Teilnehmer. Dies führte zu einer einseitigen Sprachübertragung.

→ Werden in einem Szenario mit einer übergeordneten SIP-TK-Anlage bei einem ausgehenden Telefonat in den Sitzungen zwischen Router und SIP-Client sowie Router und SIP-TK-Anlage unterschiedliche Codecs verwendet, so muss der Codec mit dem SIP-Client in einem Re-INVITE neu ausgehandelt werden, sodass der Codec übereinstimmt. Wenn die SIP-TK-Anlage in diesem Moment ein Re-INVITE zur Weiterleitung des Telefonats an den Router sendete, wurde dieses vom Router an den SIP-Client gesendet, obwohl das erste Re-INVITE noch nicht bestätigt wurde. Dies führte zu fehlender Sprachübertragung in Verbindung mit einem Rauschen bei dem anrufenden Teilnehmer.
Das zweite Re-INVITE der SIP-TK-Anlage wird jetzt erst übertragen, wenn die erste Aushandlung abgeschlossen ist.

→ Empfing der Voice Call Manager zwecks Rufweiterleitung von einer SIP-TK-Anlage an einen SIP-Client ein REFER und erhielt nach Senden eines INVITE an den SIP-Client ein ‚Session Progress' mit SDP-Daten von der SIP-TK-Anlage, sendete der Voice Call Manager zuerst ein Re-INVITE an den SIP-Client und anschließend, nach Erhalt der Meldung „200 OK" von dem SIP-Client fälschlicherweise ein ACK an die SIP-TK-Anlage, obwohl die Rufaushandlung noch offen war (ein solches Verhalten wird hauptsächlich in einem Szenario mit einer Swyx TK-Anlage in Verbindung mit einem CTI+-Client auftreten). Dies führte zu einem Abbruch des Telefonates.

→ Wurden dem Router in einem UPDATE im ‚From und Contact'-Feld von der SIP-Registrierung abweichende Parameter übermittelt, konnte der Router den SIP-Benutzer nicht zuordnen. Dies führte zu einem Gesprächsabbruch.

→ In einem SIP-Trunk-Szenario konnte es vorkommen, dass keine Rufnummerntöne an die ISDN-TK-Anlage übermittelt wurden. In der Folge konnte ein ausgehender Anruf nicht initiiert und aufgebaut werden.

LCOS-Änderungen 10.42.0383 RU2

Korrekturen / Anpassungen

Allgemein

→ An Internet-Anschlüssen der ‚Deutsche Glasfaser' wird das Router Advertisement an die Multicast-IPv6-Gruppe und die Unicast-MAC-Adresse des Routers gesendet. Dies führte dazu, dass der Router das Router Advertisement verwarf und somit keine Internet-Kommunikation möglich war. Der Router akzeptiert die Router Advertisements jetzt.

→ Beim Zurückschreiben einer Konfiguration per SSH konnte es vorkommen, dass LANconfig meldete „Die Konfiguration konnte nicht in das Gerät zurückgeschrieben werden", obwohl der Vorgang erfolgreich war.

→ Bei LANCOM Wireless ePaper Access Points (z.B. LANCOM LN-830E) konnte es vorkommen, dass die Verbindung zum Wireless ePaper Server verloren ging und nicht automatisch neu aufgebaut wurde.

→ Bei einigen LANCOM Geräten war das Herunterladen der SNMP-Geräte-MIB per WEBconfig nicht möglich.

→ Der Rückfall von IPv6 auf IPv4 funktionierte beim NTP-Client nicht korrekt.

→ Stimmte unter Verwendung des Features ‚Dynamic Path Selection' bei der Prüfung durch die Firewall das Firewall-Ziel nicht mit dem Routing-Eintrag überein, wurde die Meldung „bad gateway: <Gegenstelle A> does not match <Gegenstelle B>" ausgegeben und die nächste Firewall-Regel durchlaufen. Es konnte ebenfalls dazu kommen, dass Pakete verworfen wurden.
Es wird jetzt vor der Routen-Auswahl für die Dynamic Path Selection das Gateway der Route überprüft und die nächste Regel durchlaufen, wenn das Gateway nicht mit dem Firewall-Ziel übereinstimmt. Weiterhin wird im Firewall-Trace die Meldung „bad gateway: ACTUAL does not match REQUESTED" ausgegeben.

→ Wurde zwecks Zertifikat-Bezug per SCEP-Client der Befehl ‚do Setup/Certificates/SCEP-Client/Update' über ein Addin-Skript in der LMC auf einem Gerät ausgeführt, führte dies zu einem unvermittelten Neustart des Gerätes.

→ Es konnte bei Verwendung eines Loadbalancers vorkommen, dass dieser nach Aufbau der ersten Leitung nicht in den Status ‚connected' wechselte. Dies führte dazu, dass weitere Internet-Gegenstellen nicht aufgebaut wurden.

VPN

→ Wenn mehreren VPN-Verbindungen die gleiche Route zugewiesen wurde (z.B. per IKE-CFG Mode), wurde beim Aufbau der zweiten Verbindung die Route der ersten Verbindung in der Routing-Tabelle verdrängt. Beim Abbau der ersten Verbindung wurde die Route komplett entfernt. Dies führte dazu, dass die Kommunikation über die VPN-Verbindung zu diesem Ziel nicht mehr möglich war.

WLAN

→ IGMP-Queries von der Adresse 0.0.0.0 wurden nicht angenommen. Dies führte dazu, dass die IAPP-Tabelle leer blieb und es somit beim WLAN-Roaming zu Unterbrechungen kam.

→ Auf einem vRouter war nach einem Update auf die LCOS-Version 10.42 die Seite ‚Anmeldung (E-Mail zu SMS)' in der Public Spot-Seiten-Tabelle doppelt vorhanden und die Seite ‚Rückfall-Fehler' fehlte. Dies führte dazu, dass die Konfiguration nicht über die LMC ausgerollt werden konnte und stattdessen mit einem Fehler quittiert wurde.

→ Wenn die Public Spot-Seitentabelle im Pfad ‚Setup/Public-Spot-Modul/Seitentabelle' mit Standard-Werten gefüllt war und per LANconfig Änderungen an dieser Tabelle durchgeführt wurden, enthielt die Tabelle nach dem Zurückschreiben leere Werte mit „"-Zeichen.

VoIP

→ Die Tabelle der aktiven VoIP-Leitungen im LCOS-Pfad ‚Status/Voice-Call-Manager' zeigte maximal 32 Einträge an. Wenn mehr als 32 Leitungen aktiv waren, wurden die restlichen Leitungen nicht angezeigt. Es werden jetzt maximal 64 Einträge angezeigt.

→ Per SDP eingehende SIP-Update-Pakete wurden vom LANCOM Router ohne SDP beantwortet. In der Folge schlugen Anrufe in Verbindung mit einer nachgeschalteten TK-Anlage fehl.

→ Wenn sich während einer TTL-DNS-Periode die Prioritäten-Reihenfolge der angebotenen DNS SRV-Records änderte, wurde dies im LANCOM Voice Call Manager nicht bemerkt, sodass sich der LANCOM Router nach Ablauf der TTL nicht mit der neuen höchstgewichteten Site verbunden hat. In der Folge schlug eine SIP-Registrierung fehl.

→ Es konnte vorkommen, dass ein ISDN-Telefon die Ziel-Rufnummer (Connected Number) in einem unerwünschten Format anzeigte. Es besteht jetzt die Möglichkeit die Connected Number zu unterdrücken, sodass diese nicht in der ISDN ‚Connect Message' mitgesendet wird.

LCOS-Änderungen 10.42.0280 RU1

Korrekturen / Anpassungen

VoIP

→ Es wurden Probleme beim Vermitteln von Telefonaten mit den Methoden RE-INVITE, REFER und der damit verbundenen Voice-Codec-Aushandlung in Szenarien mit Swyx-TK-Anlagen behoben.

LCOS-Änderungen 10.42.0277 Rel

Korrekturen / Anpassungen

Allgemein

→ Anfragen von LANCOM-internen Diensten (z.B. ICMP-Anfragen oder ICMP-Messungen im DPS) ins WAN, welche eine lokale Absender-Adresse aufwiesen (z.B. ‚ping -a INTRANET 8.8.8.8'), wurden unmaskiert gesendet, wenn in der Routingtabelle ausschließlich Routen für Loadbalancer eingetragen waren und Routen für die jeweils einzelnen WAN-Verbindungen fehlten. In der Folge schlug die Anfrage fehl.

→ Das Laden einer LANCOM Routerkonfiguration von einem USB-Stick, welcher in ein unkonfiguriertes Gerät eingesteckt war, schlug fehl.

→ Der Datensatz für Netzwerke im Konsolen-Pfad ‚Status / DHCP-Client / LAN-IP-List' wurde immer mit der maximalen statt der tatsächlichen Länge angelegt.
Dies führte dazu, dass bei Auswahl eines Interfaces (z.B. INTRANET) in WEBconfig im Menü ‚Extras / LCOS-Menübaum / Status / DHCP-Client / LAN-IP-Liste / Ifc' eine leere Seite ausgegeben und die Fehlermeldung „404 Not found" angezeigt wurde. Auch per Konsole konnten die Informationen nicht ausgelesen werden.

→ Bei der Protokollierung von DNS-Auflösungen wurde das Syslog über Port 512 statt Port 514 gesendet.
In der Folge erreichten die Meldungen einen externen Syslog-Server nicht.

→ Der Voice-Call-Manager im LANCOM Router versendete E-Mails in einer Textcodierung, in welcher z.B. Umlaute unleserlich ausgegeben wurden. Die E-Mails werden jetzt UTF-8-codiert vesendet.

→ Wurde auf der Konsole ein Ping mit einer Größe kleiner als 16 Byte ausgeführt (mit dem Parameter -s), führte dies zu einem unvermittelten Neustart, da die minimale Paketgröße bei 16 Byte liegt.

→ Brauchte ein Prozess auf dem vRouter sehr lange (ausgelöst durch einen Mangel an CPU-Ressourcen), konnte dies zu einem unvermittelten Neustart führen.

→ Die Längen-Prüfung von ICMPv6-Paketen in der IPv6-Firewall funktionierte nicht korrekt. Dies konnte dazu führen, dass ICMPv6-Pakete vom Router mit der Meldung „intruder detection" verworfen wurden.

WLAN

→ Die 802.11u-Parameter ‚Include-in-Beacon-OUI' und ‚Additional-OUI' ließen auf der Konsole lediglich die Eingabe von Kleinbuchstaben zu. In LANconfig wurden für diese Parameter aber auch Großbuchstaben zugelassen. Großbuchstaben werden jetzt in Kleinbuchstaben konvertiert.

→ Bei Verwendung von 802.11u in Verbindung mit Passpoint R2 wurde der NAI-Realm nicht an das Endgerät übertragen, sodass dieses keine Verbindung aufbauen konnte.

VPN

→ Forderte der VPN-Partner mehrere Phase-1-Proposals zur parallelen Bearbeitung an statt wie sonst üblich sequenziell, kam es zu einem unvermittelten Neustart des Routers.

→ Nach einer Firmware-Aktualisierung auf LCOS 10.42 RC3 konnte es vorkommen, dass IKEv2-VPN-Verbindungen per EAP-Authentifizierung nicht mehr aufgebaut wurden, wenn in diesen kein Remote-Gateway angegeben war und als Remote-ID ‚No-Identity' verwendet wurde.

→ Nach dem Aufbau einer Dial-In-VPN-Verbindung von einer Außenstelle wurden die Routen vom annehmenden Router (Zentrale) gelöscht und direkt wieder hinzugefügt. Dies führte dazu, dass auch bestehende Sessions gelöscht wurden und die Kommunikation über diese Session nicht mehr möglich war (z.B. RDP).

VoIP

→ Sendete ein SIP-Provider ein INVITE mit einem zu kleinen Session Timer, antwortete der Router mit der Fehlermeldung „422 Session Interval Too Small". Sendete der SIP-Provider dann kein neues INVITE mit einem angepassten Session Timer, wurde das Telefonat abgebaut und der Anrufer hörte kein Rufzeichen.
Die Meldung „422 Session Interval Too Small" wird jetzt nur noch bei Verwendung einer ‚Gateway-Leitung' zur Anbindung einer SIP-TK-Anlage versendet.

→ Sendete eine SIP-TK-Anlage in der Meldung „200 OK" das Merkmal für SDP in Kleinbuchstaben (rtp/avp) an den Router, erkannte dieser das SDP nicht und sendete das „200 OK" ohne SDP an den Provider. Der Provider antwortete darauf mit einem BYE und der Fehlermeldung „488 Not Acceptable Here". Dies führte dazu, dass in einem solchen Fall das Telefonat nicht zustande kam.

→ Wenn ein SIP-Teilnehmer im INVITE in der SIP-URI das Protokoll in Kleinschreibung an den Router schickte
(z.B. udp), lehnte der Router das Paket mit der Fehlermeldung „404 Not Found“ ab.
Der Router ignoriert jetzt Groß- bzw. Kleinschreibung.

LCOS-Änderungen 10.42.0212 RC3

Neue Features

Routing & VPN

→ IPv6-Source-Adressfilter für IKEv2 VPN-Verbindungen

Korrekturen / Anpassungen

Allgemein

→ Die Tabelle für die Mobilfunk-Historie im Pfad ‚Status / Modem-Mobilfunk / Historie' blieb leer, unabhängig davon, ob eine Mobilfunk-Verbindung genutzt wurde oder nicht, da der Standardwert zur Erfassung der Historie im Pfad ‚Setup / Schnittstellen / Mobilfunk / Protokollierungsintervall' auf ‚0' (ausgeschaltet) stand. Das Standardintervall wurde nun auf 300 Sekunden (5 Minuten) geändert.

→ Die Tabelle ‚Status / Last-Admin-Logins' wies eine fehlerhafte Struktur auf, da die erste Spalte (die einzige Index-Spalte) die IP-Adresse enthielt und nicht, wie üblich, einen eindeutigen Index-Wert (z.B. eine fortlaufende Nummer).

→ Der Konfigurations-Bezug per TR-069 bei Verwendung einer IPv6-Adresse schlug fehl, da die eigene IPv6-Adresse vom TR-069-Prozess des Routers in eckige Klammern gesetzt und daher nicht korrekt erkannt wurde.
Es wurde in diesem Fall ein Fallback per IPv4 durchgeführt.

WLAN

→ In der Tabelle ‚Setup / WLAN-Management / AP-Configuration / IEEE802.11u / General' konnte für ein 802.11u-Standortprofil ein Profilname mit max. 32 Zeichen eingegeben werden. Der gleiche Parameter wurde jedoch in der Tabelle der WLAN-Profile mit einer Namenslänge von max. 31 Zeichen geführt. In der Folge konnte ein Profilname mit 32 Zeichen in der WLAN-Profil-Tabelle nicht konfiguriert werden, da die maximal zulässige Zeichenanzahl von 31 Zeichen überschritten wurde.

→ In einem WLAN-Controller-Szenario wurde die Domain ID aus dem Menü ‚WLAN-Controller / 802.11u / Hotspot 2.0 Profile' von den Access Points nicht übernommen, weshalb der Platzhalter ‚0' verwendet wurde. Dadurch wurde eine falsche Domain ID an anfragende WLAN-Teilnehmer übergeben.

→ Wurde auf einem WLAN-Controller im Konsolen-Pfad ‚Setup / WLAN-Management / AP-Configuration / IEEE802.11u / General' für den ‚Venue-Name' ein nicht unterstützter regulärer Ausdruck (RegEx) eingetragen, führte dies zu einem unvermittelten Neustart des Gerätes.

→ Bei der Verwendung einer eigenen Start-Seite im Public Spot wurde beim Aufruf derselben lediglich eine weiße Seite angezeigt, da bei der Weitergabe der Redirect-URI (Uniform Resource Identifier) an den Public Spot Teilnehmer eine falsche IP-Adresse enthalten war.

LCOS-Änderungen 10.42.0155 RC2

Neue Features

Allgemein

→ Der 802.1X-Authenticator für Ethernet-Ports ist nun in allen Geräten enthalten.
→ Der 802.1X-Authenticator kann nun optional statt einer 802.1X-Verhandlung sofort eine Prüfung der MAC-Adresse des angeschlossenen Ethernet-Geräts mit einem RADIUS-Server durchführen.
→ In Neukonfigurationen ist die MAC-Adresse von Bundle-Interfaces nun ‚0' und wird im Betrieb auf die systemweite, gerätespezifische MAC-Adresse umgesetzt. Dies erleichtert die Portierung von Konfigurationen.
→ Die HTTP(S)-Hit-Liste der Layer-7-Erkennung wurde aktualisiert.
→ Für die Verbindung mit einem Wireless ePaper-Server kann nun das ThinAP2.0/TLS-Protokoll verwendet werden.
→ In Neukonfigurationen sind die Management-Protokolle Telnet und Telnet-over-SSL nun standardmäßig deaktiviert.

Routing & VPN

→ Der Linecode des xDSL-Modems der LANCOM 179x-Serie wurde aktualisiert.

WLAN

→ Unterstützung für Stanley-AeroScout RTLS Tags
→ Besteht das Ergebnis der Kanalbeurteilung der automatischen WLAN-Kanalwahl aus mehreren gleich guten Kanälen, wird daraus ein Kanal anhand der systemweiten MAC-Adresse gewählt. Dies verbessert Szenarien, in denen mehrere benachbarte Access Points zeitgleich eine automatische Kanalwahl durchführen.
→ Unterstützung einer JSON-API zur Ausleitung von BLE- und WLAN-Lokationsdaten
→ Die standardmäßige WLAN-Passphrase ist nun leer. Zur Aktivierung einer verschlüsselten WLAN-SSID ist das Setzen einer benutzerdefinierten Passphrase notwendig.
→ Unterstützung der Konfiguration von PassPoint R2 via WLC

VoIP

→ Für SIP-Leitungen kann die Übergabe einer fixen PPI oder PAI konfiguriert werden.
→ Für SIP-PBX-Leitungen kann nun eine Loopback-Adresse konfiguriert werden.
→ Die Voice-Call-Manager-Tabelle ‚Benutzer-Einstellungen' kann nun beliebig viele Einträge beinhalten.

Korrekturen / Anpassungen

Allgemein

→ Beim LANCOM OAP-1702B fehlte im LCOS die spezifische Angabe für die PoE-Leistung, welche per LLDP bei einem PoE-fähigen Switch angefordert wurde.

→ Bei LANCOM Routern traten sporadisch CPU-Auslastungen bis zu 100% auf, welche auf ein Problem mit der Session-Anzahl in der IPv4-Maskierungstabelle der Geräte zurückzuführen waren. In der Folge kam es durch die hohe CPU-Last u.a. zu Problemen beim IPv4-Routing.

→ Die Kommunkation mit einem externen Syslog-Server über einen benutzerdefinierten Port (ungleich 514) war unabhängig vom genutzten Protokoll (TCP oder UDP) nicht möglich. Der Router ignorierte die Einstellung und nutzte weiterhin den Port 514.

→ Die Konfiguration konnte auf einen durch die LMC verwalteten Router nicht ausgerollt werden, wenn gleichzeitig ein neues Objekt in der DNS-Ziel-Liste angelegt und dieses in einer neuen Firewall-Regel referenziert wurde.

→ Wenn für einen GRE-Tunnel ein Routing-Eintrag erstellt wurde, welcher auf eine IP-Adresse aus einem lokalen Netzwerk verwies, konnte der GRE-Tunnel nicht aufgebaut werden.

→ Bei einer Änderung des Hauptgeräte-Passwortes per Konsolen-Befehl ‚passwd -n', welches das EscapeZeichen ‚\' beinhaltete, wurden weitere Zeichen vor dem Passwort eingefügt. Dies führte dazu, dass mit diesem Passwort kein Zugriff auf das Gerät möglich war und das Passwort mit dem Befehl ‚passwd -n' nicht erneut gesetzt werden konnte.

→ Es konnte bei aktivierter ‚Dynamic Path Selection' während des Ausroll-Vorgangs einer komplexen Konfiguration über die LMC zu einem unvermittelten Neustart kommen.

LCOS-Änderungen 10.42.0037 RC1

Neue Features

Allgemein

→ Die HTTP-/HTTPS-Tracking-Liste der Layer-7-Anwendungserkennung wurde aktualisiert.

Routing & VPN

→ Unterstützung für SD-WAN Dynamic Path Selection

WLAN

→ Entfall der standardmäßigen WLAN-Passphrase

→ Ein LANCOM WLC konfiguriert das erste WLAN-Modul (2,4 GHz) eines verwalteten Access Points nun per Default für 20 MHz Kanalbreite. Dies betrifft nur neu in die Verwaltung aufgenommene Access Points..

7. 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.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de