Release Notes

LCOS
10.50 RU16

Inhaltsübersicht

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 10.50 RU16sowie 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 und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, 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 in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS 10.50

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

Die Unterstützung für die folgenden Geräte entfällt ab LCOS 10.50:

- → LANCOM 1631E
- → LANCOM 1781-4G
- → LANCOM 1781A
- → LANCOM 1781AW
- → LANCOM 1781VA-4G
- → LANCOM 730-4G
- → LANCOM 7100+
- → LANCOM 9100+
- → LANCOM IAP-4G
- → LANCOM L-151
- → LANCOM L-151E
- → LANCOM L-320 R2
- → LANCOM L-330
- → LANCOM WLC-4025+
- → LANCOM WLC-4100

4. Hinweise zu LCOS 10.50

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 10.50

5.1 Feature-Highlights 10.50

Performance-Upgrade für den LANCOM ISG-8000

In großen SD-WAN- oder Standortvernetzungsszenarien mit einer Vielzahl an IPSec-VPN-Kanälen und hohem Datenaufkommen ist der Einsatz des Central Site VPN-Gateways LANCOM ISG-8000 nun noch effizienter. Durch die intelligente Verteilung der Datenlast auf mehrere Kerne (Multicore) wird die Gesamtperformance der VPN-Verbindungen auf 10 GBit/s erhöht. So können bei der Nutzung vieler VPN-Kanäle deutlich mehr Daten in kürzerer Zeit ausgetauscht werden.

Schnelles Failover für höchste Betriebssicherheit

In Infrastrukturen mit Anforderungen an höchste Betriebssicherheit sind schnelle Failover-Zeiten essenziell wichtig. Bei Einsatz von Dynamic Path Selection (DPS) oder BGP gelingt das Umschalten von einer IPSec-VPN-Verbindung zur anderen nun in weniger als einer Sekunde. Somit führt in einem Active-Active-Betrieb der Ausfall einer Verbindung zu keiner merklichen Downtime, beispielsweise bei geschäftskritischen Prozessen wie Zahlungsvorgängen mit EC-Cash-Terminals.

5.2 Weitere Features LCOS 10.50

Erweiterung der IPv6-Funktionalität

Profitieren Sie jetzt von noch mehr Zukunftsfähigkeit Ihrer IPv6-Standortvernetzung: Ab LCOS 10.50 RC1 werden Funktionen wie 464XLAT bei IPv6-only im Mobilfunk, NAT bei IPv6 (NPTv6), Load Balancing mit IPv6 sowie IPv6-Polling unterstützt.

Plattformerweiterung für den LANCOM vRouter

Für einen noch flexibleren Einsatz unterstützt der LANCOM vRouter neben den Hypervisor-Plattformen Hyper-V, ESXi und Azure jetzt auch KVM (Kernel-based Virtual Machine).

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 6 „Historie LCOS 10.50“.

6. Historie LCOS 10.50

LCOS-Änderungen 10.50.1532 RU16

Korrekturen / Anpassungen

Allgemein

→ Nachdem die maximale Anzahl der halboffenen Verbindungen für eine Verbindungs-Quelle oder ein Verbindungs-Ziel erreicht wurde, verwarf die DoS-Erkennung (Denial of Service) diese Pakete solange, bis die Laufzeit aller halboffenen Verbindungen für diese Quelle oder dieses Ziel ablief und diese gelöscht wurden. Dies konnte dazu führen, dass auch erwünschter Datenverkehr verworfen wurde.
Die DoS-Erkennung erlaubt jetzt die Kommunikation nach Überschreiten der maximalen Anzahl der halboffenen Verbindungen, wenn die Schwelle wieder zur Hälfte unterschritten ist.

→ Bei TR-069 wurden auch Verbindungsanfragen bearbeitet, deren IP-Adresse oder DNS-Name nicht in der Access Control List (ACL) vorhanden war. Es werden jetzt nur noch Verbindungen von Adressen bearbeitet, welche auch in der ACL vorhanden sind.

VPN

→ In Einzelfällen konnte es beim Aufbau / Rekeying einer Child_SA (ESP SA) auf einem LANCOM ISG-4000 / ISG-5000 / ISG-8000 sowie dem vRouter vorkommen, dass eine nicht funktionsfähige Child_SA erzeugt wurde. Dadurch konnten über den VPN-Tunnel keine Daten übertragen werden.

VoIP

→ Das SIP-ALG setzte bei abgehenden INVITEs im RTP den Media Endpoint auf 0.0.0.0. In der Folge konnte keine RTP-Session aufgebaut werden und es war keine Sprachübertragung möglich.

→ Wurde ein Anruf von einem SIP-Benutzer mit einem Ascom-Endgerät zum LANCOM Voice Call Manager gesendet und dann auf eine ISDN-Leitung weitergeleitet, konnte es nach dem Verbindungsaubau zu einseitiger Sprachübertragung kommen.

→ Versuchte ein ISDN-Teilnehmer nach einer Ruf-Weiterleitung über den Voice Call Manager das Telefonat zurückzuholen, obwohl der Voice Call Manager die Ruf-Weiterleitung eingeleitet und das Telefonat aus Sicht des ISDN-Teilnehmers somit getrennt hatte, lehnte der Voice Call Manager die Anfrage ab.
In einem solchen Fall öffnete der Voice Call Manager den Voice-Stream nicht. Dies führte zu einer einseitigen Sprachübertragung.

→ Der Voice Call Manager berücksichtigte den ‚Replaces'-Parameter im ‚To-Header' nicht. Wenn ein SIP-Telefon den ‚Replaces'-Parameter im ‚To-Header' statt in einem ‚Replaces-Header' sendete, führte dies dazu, dass das Telefonat nach dem Durchstellen eines Anrufs beendet wurde.

LCOS-Änderungen 10.50.1482 SU15

Korrekturen / Anpassungen

Allgemein

→ Es wurde eine Sicherheitslücke im Webinterface behoben, durch die unauthentifizierte Angreifer mit einem manipulierten Paket einen unvermittelten Neustart des Gerätes hervorrufen konnten (DoS-Attacke). Betroffen war der Administrations-Zugriff per WEBconfig aus dem LAN sowie aus dem WAN (sofern der Management-Zugriff für HTTP/HTTPS aus dem WAN erlaubt wurde) sowie die Web-Dienste IPSec-over-HTTPS, SCEP, OCSP-Server/-Responder und der Public Spot.
In der Standard-Konfiguration ist der Zugriff auf den Router aus dem WAN deaktiviert, wodurch der Router in diesem Fall von der Sicherheitslücke nicht betroffen war. Das Protokoll TR-069 war von der Sicherheitslücke ebenfalls nicht betroffen.

LCOS-Änderungen 10.50.1481 RU14

Korrekturen / Anpassungen

Allgemein

→ Es wurde eine Sicherheitslücke im RADIUS-Protokoll behoben (VU#456537). Für weitere Informationen beachten Sie bitte den entsprechenden LANCOM KB-Artikel.

→ Bei gleichzeitiger Verwendung von LACP und VRRP wurden die VRRP-Multicast-Pakete nicht über das LACP-Bundle übertragen. Dadurch war die Kommunikation zwischen den VRRP-Routern nicht möglich und es kam zu einem Flapping.

WLAN

→ In Szenarien, bei denen eine 802.1X-Authentifizierung für SSIDs verwendet wurde, konnten sich Clients mit Windows 11 Betriebssystem nicht mit der SSID verbinden, da die Authentifizierung fehlschlug.

VoIP

→ Empfing der Voice Call Manager eine Fehlermeldung im SIP, welche zu einem nicht mehr existierenden SIP-Call gehörte, führte dies zu einem unvermittelten Neustart des Routers.

LCOS-Änderungen 10.50.1400 RU13

Korrekturen / Anpassungen

Allgemein

→ Es wurde eine Sicherheitslücke im SSH-Protokoll behoben („Terrapin"-Sicherheitslücke/CVE-2023-48795).

→ In einem Szenario mit Config-Sync konnte es vorkommen, dass aufgrund eines fehlgeschlagenen TLS-Handshake keine Synchronisation der Konfigurationen durchgeführt wurde.

→ In einem VRRP-Szenario, in welchem für eine Gegenstelle das ICMP Line-Polling verwendet wurde, konnte es vorkommen, dass ein Rückwechsel vom Backup-Gerät zum Master-Gerät fehlschlug.

→ Nach einer Trennung der Internet-Verbindung konnte es vorkommen, dass statt der hinterlegten benutzerdefinierten MAC-Adresse die MAC-Adresse des Routers verwendet wurde.

→ Waren auf einem Router sehr viele Routing-Einträge vorhanden (z.B. per BGP gelernt) und wurden alle Interfaces durch ein Monitoring-Tool per SNMP ausgelesen (SNMP-Pfad 1.3.6.1.2.1.4.24.4, RFC 2096), wurde die CPU des Routers dadurch voll ausgelastet. Anschließend kam es zu einem unvermittelten Neustart des Routers.

→ Wurde auf einem Mobilfunk-Router mit 5G-Modul ein falscher APN eingetragen, führte dies nach einigen Minuten zu einem unvermittelten Neustart des Routers.

→ Ist kein SSL-Zertifikat für den Zugriff per Webinterface vorhanden, kann das LCOS ein temporäres Zertifikat aus dem „ssl_privkey" generieren. War in dem „ssl_privkey" ein ECDSA- statt einem RSA-Schlüssel hinterlegt, konnte kein temporäres Zertifikat erstellt werden. Dadurch war ein Zugriff per WEBconfig nicht möglich und der verwendete Web-Browser quittierte den Vorgang mit einer Fehlermeldung aufgrund eines fehlerhaften Zertifikates.

→ Wenn ein IPv6-Interface für einen EoGRE-Tunnel aktiviert wurde, konnte es vorkommen, dass sich der EoGRE-Tunnel ständig aktivierte und wieder deaktivierte (flapping).

VPN

→ Die ICMP-Polling-Funktion verwendete beim Polling-Vorgang ein falsches Routing-Tag, was bei IKEv2-Verbindungen, für welche ein Routing-Tag in der Routing-Tabelle angegeben war, dazu führen konnte, dass der Verbindungsaufbau scheiterte.

VoIP

→ Wenn in den Einstellungen einer SIP-Leitung die Verschlüsselungs-Funktion aktiviert war, funktionierte eine im Feld „SIP-Domäne/Realm“ mit dem Suffix „?6“ forcierte IPv6-Anmeldung beim Registrar nicht.

→ Wenn ein SIP-Benutzer sich ohne Transport-Parameter am LANCOM Router registriert hat, wurde ein INVITE aufgrund des fehlenden Parameters abgelehnt und ein Anruf kam nicht zustande.

→ Der Voice Call Manager unterstützt keine RTP Extensions. Empfing der Voice Call Manager ein eingehendes Telefonat mit RTP Extensions, sendete dieser die RTP Extensions auch in der „SDP Answer“ mit. Dies führte dazu, dass der angerufene Teilnehmer den Anrufer nicht hören konnte.
Der Voice Call Manager sendet im „SDP Answer“ jetzt keine RTP Extensions mehr.

→ Während eines Telefonates über den Voice Call Manager konnte es vorkommen, dass bereits reservierter Speicher überschrieben wurde. Dies führte zu einem unvermittelten Neustart des Routers.

LCOS-Änderungen 10.50.1301 RU12

Korrekturen / Anpassungen

Allgemein

→ Per WEBconfig konnte in dem Menü „Konfiguration → Routing-Protokolle → BGP → Nachbarn“ in dem Feld „Entferntes AS“ ein maximaler Wert von 2147483647 hinterlegt werden, obwohl per Konsole und per LANconfig auch höhere Werte möglich waren.

→ In Einzelfällen konnte es bei einer 802.1X-Authentifizierung von Benutzern mit dem Attribut „Framed-IP-Address“ zu einem unvermittelten Neustart des Routers kommen.

→ Nach einer undefinierten Zeit (es konnten mehrere Wochen sein) schaltete sich das WWAN-Modul selbständig ab und war dann im State „Deactivated“. In der Folge wurde eine Internetverbindung getrennt.

→ Bei Mobilfunk-Routern konnte es vorkommen, dass in der Verbindungs-Information der Mobilfunk-Verbindung („Status/Modem-Mobile/Connect-Info“) ein Fehler angezeigt wurde, obwohl die Verbindung aufgebaut war.

→ Die Ausführung eines Skripts mit den Befehlen „beginscript“ & „exit“ führte sporadisch dazu, dass bestehende BGP-Verbindungen getrennt wurden.

→ Waren auf einem Router mehrere ARF-Netzwerke mit der gleichen IP-Adresse konfiguriert (per VLAN separiert), wurde durch eine Konfigurationsänderung in den ARF-Netzwerken ein „gratuitous ARP Flooding“ in jedem Netzwerk ausgelöst. In Szenarien mit sehr vielen gleichen ARF-Netzwerken konnte dies zu starkem Paketverlust und auch zu einem unvermittelten Neustart des Routers führen.
Nach einer Konfigurations-Änderung der ARF-Netzwerke wird jetzt für jedes Netzwerk nur noch ein „gratuitous ARP“ versendet.

WLAN

→ UDP-Datenverkehr konnte auch ohne Anmeldung am Public Spot übertragen werden, sodass einige Applikationen mit ihren Servern im Internet kommunizieren konnten.

LCOS-Änderungen 10.50.1180 RU11

Korrekturen / Anpassungen

Allgemein

→ Aufgrund eines Problems bei der Initialisierung des WWAN-Moduls konnte es vorkommen, dass bei LANCOM Mobilfunk-Routern nach einer Firmware-Aktualisierung eine bestehende WWAN-Verbindung nicht mehr aufgebaut wurde.

→ Wenn in der OSPF-Konfiguration eines LANCOM Routers der Wert ‚Advertise-Default-Route' auf ‚Dynamic' eingestellt war, funktionierte das Ankündigen der Default-Route nicht, obwohl die Route in der FIB vorhanden war.

→ Die DHCPv6-Client-ID wurde bei WWAN-Schnittstellen mit dem Wert ‚0' statt mit der jeweiligen MAC-Adresse angegeben.

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

→ 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.

VPN

→ Bei der Konfiguration einer IKEv2-VPN-Verbindung auf AES-GCM wurden eingehende fragmentierte ESP-Pakete mit einer Fehlermeldung verworfen.

→ Bei Verwendung des Verschlüsselungs-Algorithmus AES-GCM wurden alle eingehenden VPN-Pakete als Fehler gezählt. Dadurch stiegen die Zähler für Rx-invalid und Rx-Errors in der VPN-Statistik immer weiter an.

→ In Einzelfällen konnte es bei einem Wechsel auf eine Backup-Verbindung vorkommen, dass die ‚Security Associations' einer VPN-Verbindung nicht abgebaut wurden. Dadurch konnte die VPN-Verbindung nicht mehr aufgebaut werden. In einem VPN-Status Trace wurde in einem solchen Fall die Meldung „VPN: local reconnect lock active" ausgegeben.

WLAN

→ Ein verwalteter Access Point verwendete nicht die im WLAN-Controller in der SSID eingetragene VLAN-ID, sondern stets die in seiner lokalen Konfiguration vorhandene VLAN-ID im Groupkey-Index. Dies führte dazu, dass Broad- und Multicasts nicht entschlüsselt und somit auch nicht übertragen werden konnten.

VoIP

→ Erhielt der Router vom SIP-Provider ein Re-INVITE mit SDP-Parametern, die der Voice Call Manager nicht verarbeiten konnte, sendete dieser statt der Meldung „488 Not Acceptable Here“ die Meldung „500 Server Internal Error“. Dadurch wurde das Telefonat vom SIP-Provider abgebaut.

→ Der Voice Call Manager leitete RTCP-Pakete einfach weiter, sodass die RTP-Header gleich blieben. Bestimmte Gegenstellen können diese Pakete nicht verarbeiten bzw. lehnen diese ab. Dies führte dazu, dass ein Telefonat nach einer Weile abgebaut wurde.
Der Voice Call Manager unterstützt jetzt RTCP, sodass die RTP-Header jetzt korrekt angepasst werden.

→ Die in der ISDN-Schnittstelle hinterlegte Vorwahl (z.B. 02405) wurde bei einer Anrufweiterleitung fehlerhaft interpretiert. Dies führte bei einem CompanyFlex-Anschluss dazu, dass in einem solchen Fall die falsche PPI in Richtung Telekom verwendet wurde. Die Anrufweiterleitung wurde dadurch abgebrochen und der Vorgang vom SIP-Provider mit der Fehler-Meldung „403 Forbidden“ quittiert.

→ Da der LANCOM Router den Parameter ‚UNENCRYPTED_SRTCP‘ nicht unterstützte, kam es bei Gesprächen nach einigen Sekunden zu einem Abbruch seitens des Providers, da die unverschlüsselten RTCP-Pakete vom SIP-Client nicht zum SIP-Provider durchgeleitet werden konnten.

LCOS-Änderungen 10.50.1107 RU10

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).

→ In Einzelfällen konnte es vorkommen, dass der DHCP-Server auf einem Router im Werkszustand (Einstellung ‚Automatisch') nicht startete und dadurch keine IP-Adresse verteilen konnte.

→ Bei einem aktiven Backup über WWAN konnte es vorkommen, dass nach einiger Zeit das Routing zwischen LAN und WAN nicht mehr funktionierte und nur durch eine Trennung der WWAN-Verbindung wieder hergestellt werden konnte.

→ Wenn ein Netzwerk-Teilnehmer im lokalen Netzwerk des Routers eine DNS-Anfrage zu schnell wiederholt, wird eine zweite DNS-Anfrage mit dem gleichen Quell-Port an den Backup-DNS-Server geschickt. Nach Erhalt der Antwort eines der beiden DNS-Server wird der Port geschlossen. Erhält der Router anschließend auch noch die Antwort des zweiten DNS-Servers, wird diese abgelehnt.
Dadurch wurde die Meldung „connection refused" im Syslog aufgezeichnet (Priorität ‚Alarm'). Durch dieses Verhalten konnte es vorkommen, dass im Syslog viele ‚False Positive'-Meldungen aufgezeichnet wurden. Die Priorität der Meldung „connection refused" wurde jetzt auf ‚Info' geändert, sodass diese in der Standard-Konfiguration nicht im Syslog aufgezeichnet wird.

→ Empfing der Router einen Broadcast für ein bestimmtes Netzwerk auf dem Interface eines anderen Netzwerks, führte dies zu einem unvermittelten Neustart des Routers, wenn in der Firewall eine Regel mit der empfangenen Broadcast-Adresse als Ziel angelegt war.

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

→ Sobald eine neue Konfiguration per Skript in einen LANCOM 1900EF-5G eingespielt wurde, verblieb das WWAN-Modem im Status ‚Device Removal / Deactivated'. Das WWAN-Modem konnte erst durch einen Neustart des Gerätes in den Aktiv-Modus versetzt werden.

→ Wenn zeitweise keine Daten über eine 4G / 5G-Internetverbindung der Deutschen Telekom übertragen wurden, konnte es vorkommen, dass die WWAN-Internetnetverbindung nach Wiederaufnahme der Datenübertragung nicht mehr funktionsfähig war.

→ Im WEBconfig-Menü ‚Setup Assistent → Public Spot Benutzer verwalten' wurden Benutzer als ‚unauthenticated' angezeigt, obwohl diese erfolgreich mit dem Public Spot verbunden waren.

→ Bei Verwendung von ICMP-Polling für eine Internet-Verbindung kam es zu einem unvermittelten Neustart des Routers, wenn eine ARP-Anfrage des Polling-Ziels beantwortet wurde, bevor die Internet-Verbindung aufgebaut war.

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

→ Bei einer aktiven Backup-WAN-Verbindung kam es ca. alle 20-30 Sekunden dazu, das für einen kurzen Moment Routing-Pakete verworfen wurden.

→ Nach Durchlauf des WEBconfig Setup-Assistenten für Telekom CompanyFlex- sowie SIP-Trunk-Leitungen deaktivierte der Assistent das Interface ‚Analog-2', obwohl hierfür eine Rufnummer hinterlegt wurde.

→ Es wurden allgemeine Verbesserungen zum Verhalten des Content-Filters im Fehlerfall (z.B. bei Nichterreichbarkeit von Rating-Servern) vorgenommen.

→ Wenn das Mobilfunk-Modul einen Netzwerk-Scan durchführte und der SMS-Dienst währenddessen auf das Mobilfunk-Modul zugriff, führte dies zu einem unvermittelten Neustart des Routers.

→ Bei Verwendung des Content Filters konnte es vorkommen, dass Proxy-Jobs beim Abbau der zugeörigen Session nicht beendet wurden und somit weiterhin Speicher belegten. Dies führte nach einiger Laufzeit des Routers zu einem unvermittelten Neustart, da kein freier Speicher mehr verfügbar war.

VPN

→ In seltenen Fällen konnnte es vorkommen, dass bei aktiver Backup-Internetverbindung über das WWAN das Routing vom LAN ins VPN nicht mehr funktionierte.

VoIP

→ 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.

→ Es konnte vorkommen, dass in der Ausgabe des Kommandozeilen-Befehls „show vcm" die TTL-Angabe in hexadezimaler Form dargestellt wurde.

→ Die Änderung des Passwortes eines Public Spot-Benutzers in WEBconfig funktionierte nicht. Nach der Änderung konnte das neue Passwort nicht zur Anmeldung am Public Spot verwendet werden.
Wenn die E-Mail-Adresse in einem neu erstellten Benutzerkonto identisch mit der eines bereits bestehenden Kontos war, die Groß- / Kleinschreibung jedoch unterschiedlich, wurde ein neues Benutzerkonto angelegt, obwohl es sich um die gleiche E-Mail-Adresse handelte.

→ Aufgrund einer ungünstigen Reihenfolge bei der LANCOM-internen Suche nach konfigurierten SIP-Leitungen konnte es vorkommen, dass dynamische SIP-Leitungen nicht gefunden wurden.

→ Bei einer sehr schnellen Anrufannahme seitens eines ISDN-Telefons konnte es vorkommen, dass der Voice Call Manager das ‚200 OK' vor dem ‚PRACK' des SIP-Providers sendete. Das Telefonat wurde dadurch abgebaut.

→ 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' an den 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.

→ Aufgrund einer ungünstigen Reihenfolge bei der LANCOM-internen Suche nach konfigurierten SIP-Leitungen, konnte es vorkommen, dass dynamische SIP-Leitungen nicht gefunden wurden.

→ Bei einer sehr schnellen Anrufannahme seitens eines ISDN-Telefons konnte es vorkommen, dass der Voice Call Manager das ‚200 OK' vor dem ‚PRACK' des SIP-Providers sendete. Das Telefonat wurde dadurch abgebaut.

LCOS-Änderungen 10.50.1050 RU9

Neue Features

→ Das ‚loadfirmware'-Kommando auf der CLI wurde um den Schalter ‚-e' ergänzt, bei dem die Firmware zuerst heruntergeladen, im Flash temporär zwischengespeichert und danach installiert wird.

Korrekturen / Anpassungen

Allgemein

→ Nach einem WWAN-Netzwerkscan wurde in der Tabelle ‚Status/Modem-Mobile/' statt des Wertes ‚5G' die Zahl ‚12' angezeigt.

→ 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.

→ Erfolgte ein in einem VRRP-Szenario 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 Verwendung einer L2TPv3-Verbindung funktionierte die PMTU-Discovery nur, wenn dem Interface eine IP-Adresse zugeordnet war. In Szenarien, bei denen dem Interface keine IP-Adresse zugeordnet werden konnte, oder dies nicht sinnvoll war, führte dies zu Performance-Einbrüchen, wenn Pakete wiederholt übertragen werden mussten.
Die PMTU-Discovery wird jetzt auch in Szenarien ohne zugewiesene IP-Adresse unterstützt.

→ In der WEBconfig-Oberfläche eines Gerätes der LANCOM 19xx-Serie wurde für eine funktionsfähige zweite VDSL-Verbindung auf der Schnittstelle ‚VDSL-2'/'XDSL-2' beim Interface ‚VDSL-2-1'/'XDSL-2-1' der Status „interner Fehler" angezeigt.

→ Das TR069-Protokoll funktionierte nicht über beliebige Mobilfunk-Internetverbindungen. Über den Provider ‚Deutsche Telekom' ist TR-069 über Mobilfunk weiterhin nicht möglich.

VPN

→ Wenn das Rekeying einer Phase-2-SA mit anderen Crypto-Parametern als bei der ersten Phase-2-SA erfolgt, wird weiterhin der IPSec-Transport der bisherigen Phase-2 verwendet. Wurde die Verschlüsselung in einem Fall in Hardware und in dem anderen Fall in Software umgesetzt, führte dies zu einem unvermittelten Neustart des Routers.

WLAN

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

VoIP

→ 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 anstatt 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.

→ Wenn TR069-Einstellungen nach der Gerätekonfiguration geändert werden, wird diese Änderung im ACS-Bereitstellungscode widergespiegelt, der mit dem ACS-Server zurück synchronisiert werden muss. Der Synchronisierungsvorgang wurde jedoch nicht ausgeführt, sodass z.B. geänderte Firmware-Update-Einstellungen nicht laut Änderung durchgeführt wurden.

→ Die Registrierung eines VoIP-Clients an einer übergeordneten PBX wurde vom Voice Call Manager des LANCOM Routers sporadisch getrennt. In der Folge verlor der analoge Client seine Verbindung zur PBX bis zur nächsten erfolgreichen Re-Registrierung.

→ 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 anstatt den bisherigen Header zu übernehmen. Dies führte dazu, dass das Telefonat durch den SIP-Provider abgebaut wurde.

→ Initiert ein Analog- oder ISDN-Benutzer an einem LANCOM Router ein ausgehendes Telefonat, verwendet der Voice Call Manager eine Codec-Liste mit PCMA und danach PCMU. Schlug die Gegenseite ebenfalls eine Liste mit beiden Codecs in umgekehrter Reihenfolge statt eines konkreten Codecs vor, verwendete der Voice Call Manager für die RTP-Kommunikation den Codec PCMA. Wenn die Gegenseite die RTP-Kommunikation per PCMA nicht zuließ, führte dies dazu, dass die Sprachübertragung nicht funktionierte.
Bei Erhalt einer Codec-Liste verwendet der Voice Call Manager jetzt immer den ersten Codec.

→ Empfing der Voice Call Manager bei einer Rufweiterleitung im Provisional Response (181 Call is being forwarded) einen Route-Header, wurde dieser vom Voice Call Manager im nachfolgenden PRACK an den SIP-Provider nicht mitgesendet. Dies führte dazu, dass der SIP-Provider das Telefonat mit der Meldung „481 Call Leg/Transaction Does Not Exist“ abbaute.

LCOS-Änderungen 10.50.0953 RU8

Neue Features

→ DNS-Weiterleitungen in der Tabelle ‚Weiterleitungen' werden nun auch auf LAN-Interfaces unterstützt, nicht nur auf Gegenstellen. Dazu muss auf dem entsprechenden LAN-Interface ein DNS-Server per DHCP bezogen worden sein.

→ Die Behandlung von ARP bei Bridge-Schnittstellen ist nun schaltbar.

Korrekturen / Anpassungen

Allgemein

→ Aufgrund eines Fehlverhaltens des DNS-Caches 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.

→ Beim LANCOM vRouter wurde die Angabe des zur Verfügung stehenden Arbeitsspeichers (RAM) nicht korrekt wiedergegeben.

→ Im Syslog von LANCOM Mobilfunk-Routern der 19xx-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 in dem Pfad ‚Setup/Certificates/SCEP-CA/Web-Interface/Profiles/' das Zeichen „/" hinterlegt werden.

→ RIP-Netzwerke werden in einer Tabelle nachgehalten, um zu prüfen, ob sich die Quelladresse in dem hinterlegten Netzwerk befindet. Bei einem ‚Link Down'-Event wird das Netzwerk aus der Tabelle entfernt und bei einem ‚Link Up'-Event wieder in die Tabelle eingefügt. Nach einem ‚Link Down'- und anschließendem ‚Link Up'-Event konnte es vorkommen, dass das Netzwerk nicht wieder in die Tabelle eingefügt wurde. Weiterhin wurde das Netzwerk nach einem Neustart des Routers nicht in die Tabelle aufgenommen, wenn die Funktion ‚Dieses Netz in anderen Netzen via RIP bekanntgeben' nicht aktiv war.
In beiden Fällen führte dies dazu, dass das RIP-Netzwerk nicht propagiert wurde. In einem RIP-Trace wurde dann die Fehlermeldung „bad source IP

address → discard“ ausgegeben.

→ Das Deaktivieren der Funktion TR-069 durch einen ‚Auto Configuration Server‘ (ACS) eines Internet-Providers wurde nicht bootpersistent gespeichert.

→ Der NTP-Client führte beim NTP-Abgleich die DNS-Auflösung immer explizit mit IPv4 UND IPv6 durch, wodurch der fortlaufende Abgleich fehlschlagen konnte, wenn z.B. IPv6 nicht verwendet wurde. Die DNS-Auflösung wird nun immer mit IPv4 ODER IPv6 durchgeführt.

→ In einem Szenario aus Internet-Verbindung mit Backup und VPN-Verbindung mit Backup erfolgte nach einem Ausfall der Internet-Verbindung ein Schwenk auf die Backup-Verbindung. Dadurch wurde auch der Aufbau des VPN-Backups iniitiert. 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‘).

→ Bei 5G-WWAN-Verbindungen im Standalone-Modus fehlten nach einem erfolgreichen Verbindungsaufbau die Informationen zum Funkmodus und zu den verwendeten Frequenzbändern.

→ Ein DNS-Check für einen DynDNS-Eintrag in der Aktionstabelle funktionierte nicht, wenn dieser DNS-Name auch im lokalen Netzwerk vorhanden war.

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

→ Nach dem Neuaufbau einer bestehenden 464XLAT-Verbindung, welche das PLAT-Präfix via DNS-Record gelernt hatte, wurde anschließend keine neue DNS-Anfrage für das PLAT-Präfix gestellt.

→ Aufgrund eines Fehlers in der Erkennung von konfigurierten WWAN-Verbindungen (4G/5G) bei Dual-SIM-fähigen LANCOM Routern (z.B. LANCOM 1906VA-4G) konnte es vorkommen, dass im WEBconfig-Dashboard der Geräte auch Verbindungen als aktiv angezeigt wurden, welche nicht konfiguriert waren.

→ 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.

→ 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.

→ Es konnte keine ‚5G Standalone‘-Verbindung über 5G-Router aufgebaut werden (für den ‚5G Standalone‘-Betrieb wird mindestens die WWAN-Firmware 03.09.06 benötigt).

→ Erfolgte nach dem Pairing eines Gerätes mit der LMC bei aktiver Übernahme von manuellen Konfigurationsänderungen in die LMC eine fehlerhafte Konfiguration per LANconfig (etwa ein Verweis auf ein nicht existentes Profil), wurde die Konfiguration bei einem Firmware-Update nicht korrekt konvertiert und diese daher in der LMC anschließend als ‚Nicht Aktuell' bezeichnet. Dies führte bei einem weiteren Firmware-Update zu einem unvermittelten Neustart des Gerätes.

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

→ Wenn man über die Kommandozeile eines LANCOM Routers per LL2M mit einem anderen LANCOM Gerät verbunden war und in der Session ein Skript auf das andere Gerät schrieb, startete der Router, von dem die LL2M-Verbindung initiiert wurde, unvermittelt neu.

→ Bei Routern mit 5G-Modem wurde der Datendurchsatz nicht angezeigt und verblieb dauerhaft auf 0.

→ Wenn im Secure Terminal der LMC ein Befehl eingegeben wurde, konnte es sporadisch vorkommen, dass das erste Zeichen des abgesetzten Befehls fehlte.

VPN

→ OpenSSL konnte bestimmte Parameter in der X509v3-Extension nicht verarbeiten. Nach dem Hochladen eines entsprechenden VPN-Zertifikates konnte es zu einem unvermittelten Neustart des Routers kommen.
Weiterhin konnte es ebenfalls zu einem unvermittelten Neustart des Routers kommen, wenn ein solches Zertifikat in einem VPN-Client für eine IKEv2-Authentifizierung mit dem Router verwendet wurde, das Zertifikat aber nicht im Router hochgeladen war.

→ 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.

WLAN

→ Wenn in einem per WLC verwalteten WLAN die Client-Steering-Funktion verwendet wurde und viele WLAN-Clients an einer SSID angemeldet waren, konnte es zu einem unvermittelten Neustart des WLC kommen.

→ Wurden auf einem WLAN-Controller in dem verwendeten WLAN-Profil die IP-Adressen zusätzlicher WLAN-Controller (IP-Adr. alternativer WLCs) mit einem Wert >= 128 in einem Oktett hinterlegt, wurden diese in einem CAPWAP-CTRL Trace im ‚Discovery Response' fehlerhaft angezeigt.
→ Wenn in einem WLC-Szenario bei einem über SSH verbundenen LANCOM Access Point mit aktiviertem VLAN-Modul ein Eintrag in die Tabelle ‚Setup/WLAN-Manangement/Static-WLC-Configuration' hinzugefügt oder entfernt wurde, konnte dies zu einem Verbindungsverlust zwischen dem WLC und dem Access Point führen.
→ Wenn für einen bestimmten Access Point eine Funkfeld-Optimierung durchgeführt werden sollte (per Angabe des Gerätenames oder der MAC-Adresse), so schlug die Optimierung fehl.

VoIP

→ Aufgrund einer fehlerhaften Behandlung von Informationen in den RTP-Streams eingehender FAX-Übertragungen konnte es vorkommen, dass diese abbrachen.
→ Wenn bei aktivem SIP-ALG ein SIP-Client im lokalen Netzwerk die IP-Adresse des SIP-Registrars änderte, verwendete der SIP-ALG weiterhin die alte IP-Adresse. Dies führte dazu. dass der SIP-Client die Registrierung verlor und dadurch keine Telefonate mehr möglich waren.
→ Wenn der primäre SIP-Server nicht erreichbar ist, erfolgt automatisch ein Wechsel auf den nächsten verfügbaren Server. Der Voice Call Manager blieb anschließend dauerhaft (somit auch nach Ablauf der TTL) mit diesem Server verbunden und wechselte nicht wieder auf den primären Server zurück, es sei denn, die Server-Reihenfolge änderte sich.
→ 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 anstatt 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.
→ Wenn bei einem SIP-Einzelaccount im INVITE eines ausgehenden Anrufes eine falsche PPI hinterlegt war (z.B. falsches Format) wurde der Ruf seitens des Registrars abgelehnt und kam in der Folge nicht zustande.

LCOS-Änderungen 10.50.0819 RU7

Neue Features

→ Unterstützung eines DHCPv4 Stateless Relays

Korrekturen / Anpassungen

Allgemein

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

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

→ Wenn die TR069-Funktion durch den ACS-Server deaktiviert wurde, stoppte die Kommunikation zwar wie gewünscht, nach einem Neustart des Routers wurde TR069 jedoch wieder ausgeführt, da die Funktion wieder aktiv geschaltet war.

→ Bei einem LANCOM ISG-8000 fehlte im Konfigurationspfad ‚/setup/lan-bridge' die Tabelle für die Auswahl der zu verwendenden Kommunikations-Protokolle.

→ Wenn im WEBconfig die Option ‚Extras/LCOS-Menübaum/Setup/Config/Passwörter/Klartext-behalten' auf den Wert ‚Nein' eingestellt wurde, konnte es zu einem unvermittelten Neustart des Gerätes kommen.

→ Wenn die Länge eines Konsolen-Pfads 100 Zeichen überschritt, führte dies bei Speicherung der Konfiguration als Skript zu einem unvermittelten Neustart (da Wörter auf Deutsch in der Regel mehr Zeichen haben als die englische Bezeichnung, kann dies bei Umstellung der Konsolen-Sprache auf Deutsch häufiger auftreten).
Die maximale Zeichenlänge eines Konsolen-Pfades wurde jetzt angehoben.

→ Bei gleichzeitiger Verwendung von Hairpin-NAT und Policy-Based-NAT funktionierte Policy-Based-NAT nicht mehr, wenn eine Hairpin-NAT Session beendet wurde. In einem Firewall-Trace wurde in diesem Fall die Fehlermeldung „inbound masquerading, packet rejected" ausgegeben.

→ Es konnte auf einem LANCOM ISG-8000 sporadisch zu unvermittelten Neustarts kommen, da die Multicore-Unterstützung einen Fehler aufwies.

→ Eine im Konsolen-Pfad ‚Setup/Autoload/Network/Firmware' hinterlegte Loopback-Adresse wurde nicht berücksichtigt. Dies konnte dazu führen, dass der Download-Server nicht erreicht und somit das Firmware-Update nicht durchgeführt werden konnte.

WLAN

→ Wenn in der Konfiguration eines LANCOM WLAN-Controllers im Menü ‚WLAN-Controller/AP-Konfiguration/IP-Parameter-Profile' 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.

→ Bei Verwendung eines WLC-Tunnels müssen Datenpakete eine Größe 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 LCOS LX Access Points dazu, dass diese die entsprechenden Datenpakete nicht verarbeiten konnten und die Pakete somit verworfen wurden.

VoIP

→ Der WEBconfig Setup-Assistent zur Konfiguration eines All-IP-Anschlusses legte die Konfiguration von analogen Benutzern nicht korrekt an. Es wurde bei den Benutzereinträgen nur beim ersten Eintrag eine korrekte Angabe für das zu nutzende Interface (z.B. Analog-1) hinterlegt.

LCOS-Änderungen 10.50.0725 RU6

Neue Features

→ 5G-Performance-Verbesserungen für LANCOM 1926VAG-5G und 1900EF-5G

→ Neuer DSL-Linecode für die LANCOM 179x-Serie mit Unterstützung für die DSL-Features ‚Save our Showtime' (SOS) und ‚Robust Overhead Channel' (ROC) zur Verbesserung der Stabilität an DSLAMs, die diese optionalen Features unterstützen

→ Die TR-069 TLS-Defaultwerte wurden auf aktuelle Verschlüsselungs-algorithmen angepasst.

→ Verbesserungen bzgl. der Synchronisierung zwischen der LANCOM Management Cloud (LMC) und TR-069

Korrekturen / Anpassungen

Allgemein

→ Nach einer Aktualisierung auf LCOS 10.50 RU5 fehlte in der Konfiguration eines LANCOM 1783VA-4G im Pfad ‚/Setup/Interfaces/Mobile' die Funktion ‚Enable-HSUPA'.

→ 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.

→ Wurde in der Tabelle ‚/Setup/Interfaces/DSL' eine Bandbreitenbegrenzung von mehr als 4 GBit/s eingetragen, kam es zu einem Überlauf, da in der Tabellenspalte maximal 32 Bit-Werte eingetragen werden konnten. Dies wurde nun auf 64 Bit geändert.

→ Bei Internetverbindungen auf Geräten der LANCOM 1926-Serie konnte es in unregelmäßigen Abständen zu Abbrüchen und Sync-Verlusten kommen, wenn seitens des Providers häufige Anpassungen der Datenraten vorgenommen wurden (z.B. aufgrund von Schwankungen des Störabstands auf der xDSL-Leitung).

VoIP

→ 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 im Feld für die PAI oder PPI eine Nummer vorhanden, die aber nicht mit dem konfigurierten SIP-Benutzer übereinstimmte, 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.

LCOS-Änderungen 10.50.0619 RU5

Neue Features

→ Der USB-Drucker-Server ist nach einem Geräte-Reset im Default deaktiviert.

→ Der Netzwerkname kann nun bei den Aktionstabellenvariablen für IPv6 LAN-Adresse und LAN-Präfix (%x und %y) angegeben werden.

Korrekturen / Anpassungen

Allgemein

→ 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.

→ Bei Verbindungsaufbau einer VPN-Verbindung über das 5G-Modul (WWAN) eines LANCOM 1926VAG-5G oder 1900EF-5G war keine Kommunikation über die VPN-Verbindung möglich.

→ Ein DynDNS-Abgleich über die Aktionstabelle per IPv6 war nicht mit einem statischen Präfix möglich. Weiterhin funktionierte der DynDNS-Abgleich nur für das Netzwerk INTRANET, nicht aber für andere Netzwerke.

→ Auf einem vRouter sowie auf dem LANCOM ISG-8000 wurde die ‚Checksum Offloading Info' immer hinzugefügt, auch wenn dies nicht erforderlich war. Dies konnte bei mit einem VLAN-Tag versehenen Paketen dazu führen, dass diese nicht übertragen werden konnten.

→ 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.

VPN

→ Für ein Interface mit noch nicht ausgehandelter MTU wurde ein Standard-Wert von 1280 Bytes verwendet. Da die Anpassung an die MTU nicht korrekt funktionierte, wurde weiterhin der Standard-Wert von 1280 Bytes verwendet. Dies führte dazu, dass größere Pakete mit gesetztem ‚Don't fragment' Flag über eine VPN-Verbindung nicht übertragen werden konnten und die Kommunikation somit stark gestört oder nur sehr langsam möglich war.

VoIP

→ Wenn der LANCOM VoIP-Router einen Anruf empfing, der optionale Angaben zur verwendeten Bandbreite der Session enthielt, kopierte er diese Zeilen doppelt in die Antwort „200 OK", welche er beim Annehmen des Anrufs sendete. In der Folge kam ein eingehender Anruf nicht zustande.

→ Bei der Verwendung von SNOM DECT-Endgeräten konnte es vorkommen, dass diese sich nicht mehr am LANCOM Router registrieren konnten, da Geräte die ‚Contact URI' bei jedem Registrierungsvorgang veränderten und die im REGISTER gesendete Änderung nicht in der gespeicherten Binding-Information des LANCOM Routers geändert wurde.

→ 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.

→ 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.

→ Wenn der SIP-Provider eine Änderung der Priorität der SIP-Server in einem SRV-Response ankündigte, wurde die SIP-Leitung abgebaut und im Syslog die Meldung „generic failure“ ausgegeben.
Die SIP-Verbindung wird jetzt nur noch dann ab- und neu aufgebaut, wenn die IP-Adresse des aktuell verwendeten SIP-Servers nicht mehr der IP-Adresse des höchst-priorisierten Servers entspricht. In diesem Fall wird im Syslog die Fehlermeldung „server order changed“ ausgegeben.

LCOS-Änderungen 10.50.0530 RU4

Neue Features

→ Für den 802.1X-Authenticator für LAN-Verbindungen lässt sich nun ein getrennter RADIUS-Server für den MAC-Authentisierungs-Bypass angeben.

Korrekturen / Anpassungen

Allgemein

→ Eine Änderung der Übertragungs-Betriebsart in der WWAN-Konfiguration eines LANCOM 5G-Routers hatte keine Auswirkung. Es wurden immer alle möglichen Betriebsarten verwendet.

→ Wenn der PPTP-, PPPoE- oder der L2TP-Server aktiv war und gleichzeitig der Fernzugriff auf den Router erlaubt wurde, kam es bei einem Verbindungsaufbau-Versuch auf den Router unter Verwendung des Benutzernamens ‚admin' zu einem unvermittelten Neustart, welcher durch das Schreiben des Event-Logs ausgelöst wurde.

→ Beim Aufruf von HTTPS-Webseiten durch das Feature ‚Dynamic Path Selection' verwarf der HTTP-Client im Router die HTTPS-Sessions nicht und gab auch den Speicher nicht wieder frei. Dies führte nach einiger Laufzeit zu einem unvermittelten Neustart des Routers, wenn kein freier Speicher mehr zur Verfügung stand.

→ In Einzelfällen konnte es zu einem unvermittelten Neustart des Routers kommen, wenn eine interne IPSec-Tabelle noch nicht korrekt initialisiert war und ein IPSec-Paket empfangen wurde.

→ Nach Anpassung der Schlüssellänge einer bestehenden Zertifizierungsstelle (CA) konnte diese anschließend nicht neu initialisiert werden, da aufgrund der unterschiedlichen Schlüssellänge die CA nicht gestartet werden konnte.

→ 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.

WLAN

→ Bei einem LANCOM ISG-8000 mit aktivierter Public Spot-Option lag die maximale Anzahl der unterstützen Public Spot-Benutzer anstatt der unbegrenzten Benutzeranzahl (empfohlen werden maximal 2500 Nutzer) bei 128 Benutzern.

→ Nach der Durchführung eines Umgebungs-Scans zur Erkennung von Rogue Access Points verblieb das jeweilige WLAN-Modul im Scan-Modus. In der Folge konnte der normale WLAN-Betrieb auf dem Modul nicht verwendet werden.

→ Bei Verwendung eines WLAN-Interfaces im P2P-Modus verwendet dieses als BSSID die MAC-Adresse der WLAN-Karte, und den logischen WLAN-Interfaces werden lokale MAC-Adressen als BSSID zugewiesen.
Wenn die P2P-Konfiguration per Addin-Skript über die LMC ausgerollt wurde, konnten die Aktionen für die Zuweisung der MAC-Adressen nicht korrekt initiiert werden und somit erhielten das P2P-Interface und die weiteren logischen WLAN-Interfaces die gleiche BSSID. Dies führte zu einem unvermittelten Neustart des Access Points. Weiterhin wurde die P2P-Konfiguration nicht übernommen.
→ Das Zeichen ‚ALT+34' konnte bei der Vergabe eines WPA-PSK nicht verwendet werden.

VoIP

→ Das ‚#'-Zeichen wird im ASCII-Zeichensatz mit ‚%23' codiert. Wenn in einer Call-Route eine Filterung der gerufenen Nummer z.B. mit ‚#21#' verwendet wurde, im ‚To'-Header des entsprechenden INVITE jedoch die Zeichenfolge ‚%2321%23' angegeben war, wurde das Invite falsch bearbeitet und ein Anruf kam nicht zustande, da die Zeichenfolge ‚%23' nicht als nur ein Sonderzeichen, sondern als drei Zeichen behandelt wurde. Im LANCOM Router erfolgt daher nun immer zunächst eine Umwandlung von ‚%23' in ‚#' und später (aus Kompatibilitätsgründen) zurück zu ‚%23'.
→ Der Voice Call Manager handelt mit dem SIP-Provider einen Wert für die Aktualisierung der Registrierung (Min-Expires) aus und verwendet diesen.
In Szenarien, in denen der SIP-Provider im „200 OK" nach dem REGISTER im Contact Feld einen kleineren ‚Expires'-Wert vorgab, wurde dieser vom Voice Call Manager nicht berücksichtigt. Dies führte dazu, dass die Registrierung nach Ablauf des ‚Expires'-Wertes abbrach.

LCOS-Änderungen 10.50.0434 RU3

Neue Features

→ Der Status der IPv6-Firewall wird nun im WEBconfig-Dashboard angezeigt.

→ Bei Logins bzw. Login-Versuchen auf das Gerät wird nun auch die MAC-Adresse (falls verfügbar) der zugreifenden Station protokolliert.

→ Mit LCOS 10.50 RU3 wird eine aktualisierte Modem-Firmware für die DSL-Modems der LANCOM 1926-Serie bereitgestellt, welche Stabilitätsverbesserungen für G-FAST und VDSL-Verbindungen enthält.

Korrekturen / Anpassungen

Allgemein

→ In der Kommandozeile war beim Befehl ‚ls' eine Filtermöglichkeit per @-Zeichen nicht mehr möglich (z.B. ls Status/Voice-Call-Manager/Lines/ @ „WIZ_T-123456").

→ Wenn beim Login auf ein LANCOM Gerät mit dem Benutzerkonto des Root-Administrators kein Benutzername angegeben war, wurde im Event-Log des Gerätes auch kein Benutzername in den jeweiligen Log-Eintrag geschrieben.

→ 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.

→ Ein Zugriff per LL2M auf ein Gerät im Werkszustand ohne gesetztes Passwort war nicht möglich. In diesem Fall wurde die Fehlermeldung „user unknown on remote system" ausgegeben.

→ 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 ein Client eine NAPTR-Anfrage an den Router stellte, kam es mit LCOS 10.50 und aktivierter DNS-Protokollierung im Syslog-Server zu einem unvermittelten Neustart des Routers.

VPN

→ Wenn in der Tabelle für weitere entfernte VPN-Gateways ein Eintrag mit einem Routing-Tag angegeben war, für welches es keine Route in der IP-Routing-Tabelle gab, wurde eine VPN-Verbindung bei Nichterreichbarkeit des primären entfernten Gateways auch dann nicht aufgebaut, wenn in der Tabelle ‚Weitere entfernte Gateways' Einträge mit einem Routing-Tag vorhanden waren, für das eine Route existierte.

WLAN

→ 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.

→ Wurden auf einem Access Point mit aktiver DSLoL-Verbindung größere Datenmengen übertragen (etwa durch einen Download oder einen längeren Speedtest), konnte dies zu einem unvermittelten Neustart des Access Points führen.

VoIP

→ Wurde in einem Szenario mit einer SIP-TK-Anlage ein Telefonat zwischen zwei Teilnehmern (A und B) mittels der Funktion ‚Halten' an einen dritten Teilnehmer (C) weitergeleitet, beantwortete der LANCOM Router das INVITE (ohne SDP) der TK-Anlage selbst, statt dieses weiterzuleiten. Dies führte dazu, dass anschließend keine RTP-Daten übertragen wurden und somit keine Sprachübertragung zwischen den Teilnehmern A und C möglich war.

→ Bei ausgehenden Anrufen an ein Fax-Endgerät konnte es wegen einer „403 Error Response" auf das Re-INVITE mit dem Text „Forbidden - PBX Validation Failed" sporadisch zu einem unvermittelten Neustart des LANCOM Routers kommen, wenn auf dem LANCOM Router die Overlap-Dialing-Funktionalität verwendet wurde.

→ 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.

→ Es konnte beim Versand eines SNMP-Traps mit Informationen zu ISDN-Benutzern zu einem unvermittelten Neustart des Routers kommen.

LCOS-Änderungen 10.50.0331 RU2

Neue Features

→ Unterstützung für das Modul LANCOM SFP-GPON-1

→ Aktualisierung des DSL-Linecodes der LANCOM 1926er-Serie

Korrekturen / Anpassungen

Allgemein

→ Durch eine fehlerhafte 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.

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

→ Bei den LANCOM Routern der 1926er-Serie konnte es zu regelmäßigen Abbrüchen der ADSL- und/oder VDSL-Internetverbindung kommen. Die Internetverbindungen wurden nach einem Abbruch auch nicht automatisch wieder aufgebaut (Neustart behob das Problem bis um nächsten Abbruch).

→ Bei aktivierter TR-069-Funktionalität konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.

→ Aufgrund eines eingeschränkten Zeichenumfangs konnten bei BGP keine IPv6-Link Local-Adressen verwendet werden.

→ Wenn in der Konfiguration eines LANCOM Routers ein IPv4-Adress Pool hinterlegt war und über den Setup-Assistent im WEBconfig eine neue VPN-Einwahl erstellt wurde, konnte der bereits vorhandene Adress-Pool im Setup-Assistent nicht ausgewählt werden.

WLAN

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

VoIP

→ 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 10.50.0235 RU1

Neue Features

→ Der Aktivitätsstatus des DNS-Forwarders wird nun auch im WEBconfig-Dashboard unter ‚Dienste' angezeigt.

→ **VoIP:** Für TCP-basierte SIP-Leitungen wird nun alle 60 Sekunden ein TCP-Keepalive-Paket gesendet. Das Intervall ist auf der CLI konfigurierbar.

Korrekturen / Anpassungen

Allgemein

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

→ Beim Abspeichern einer Skript-Konfigurationsdatei in WEBconfig wurde der Datei eine ungültige Dateiendung zugewiesen.

→ Bei Eingabe des Befehls ‚show ip-addresses' blieb der Wert für die DHCP-Lease-Time, wenn er den Wert 0 erreicht hatte, auf diesem Wert stehen.

→ 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.

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

→ Bei Verwendung bestimmter DSLAMs auf der Provider-Seite 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.

→ Wenn ein LANCOM Router als DNS-Server betrieben wurde, antwortete das Gerät bei SOA- und NS-Anfragen in einigen Fällen mit der Trace-Meldung „bad coded request". In der Folge konnte die Anfrage nicht ausgeführt werden.

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

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

→ Bei Verwendung einer Loopback-Adresse für den E-Mail-Versand per SMTP wurde die Loopback-Adresse nicht berücksichtigt. Wurde in der Loopback-Adresse ein Routing-Tag abweichend von 0 angegeben, fand für dieses keine Übergabe an den SMTP-Dienst statt und es wurde das Routing-Tag 0 verwendet. Dies konnte dazu führen, dass der E-Mail-Versand nicht möglich war.

→ Aufgrund einer Limitierung in der Anzahl der angemeldeten MAC-Adressen konnte die VRRP-Funktion nur auf den ersten 6 ARF-Kontexten verwendet werden. Dies betraf nur Router mit DPAA (19xx-Serie, ISG-1000, ISG-4000 und WLC-1000.

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

→ 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.

→ Der Abgleich der IP-Adresse mit einem DynDNS-Dienst funktionierte bei Verwendung von HTTPS nicht, da der Datenverkehr aufgrund einer zu hohen MTU nicht übertragen werden konnte.

→ Pakete aus einem Netzwerk mit zugeordneter LACP-Schnittstelle wurden durch die Firewall verworfen, da die Intruder Detection ein falsches Interface erkannte. In der Folge war die Kommunikation mit diesem Netzwerk nicht möglich.

→ Wenn in der Backup-Tabelle eine Backup-Verbindung angegeben wurde, deren Namensbezeichnung kürzer war, als die der Haupt-Verbindung, konnte eine Firewall-Regel, welche ein Stations-Objekt mit der Namensbezeichnung der Haupt-Verbindung enthielt, nicht in das Gerät geschrieben werden.

→ Es konnte bei Verwendung von LACP sporadisch vorkommen, dass die Antwort auf ein eingehendes Paket über eine andere LACP-Schnittstelle gesendet wurde. Dies führte dazu, dass das Paket verworfen wurde.

→ Auf Routern mit Hardware-Switch (17xx- und 19xx-Serie) wurde in diesem Fall im Ethernet-Trace die Fehlermeldung „sEthSwitchDrvrDscr: WARNING: physical port x is not part of function LAN-x (port mask 0×04), packet will be discarded" ausgegeben. Auf Routern ohne Hardware-Switch (ISG-x000, vRouter) wurden die Pakete stillschweigend verworfen.

WLAN

→ Access Points mit einer alten Firmware (z.B. Version 9.24) konnten aufgrund einer fehlerhaften TLS-Aushandlung nicht von einem WLAN-Controller verwaltet werden.

→ 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.

→ Nach einem Firmware-Update auf LCOS 10.50 konnte es bei einem OAP-830 ohne aktive VPN-Option in Einzelfällen zu einer Bootschleife kommen.

→ Wenn bei gesetzter WLAN-Trace-MAC-Adresse ein WLAN-Strength-Trace ausgeführt wurde, kam es zu einem unvermitteltem Neustart des Gerätes.

VoIP

→ Bei Szenarien, in welchen ein Swyx-Server mit einer Software kleiner als Version 12.30 verwendet wurde, konnte die Fax-Übertragung vom LANCOM Router zu Swyx aufgrund einer fehlerhaften Transaction-ID fehlschlagen.

→ Da vom LANCOM Voice Call Manager gesendete TCP-Keepalive-Pakete ein SYN-Flag enthielten, konnte es vorkommen, dass VoIP-Leitungen, bei denen keine Signalisierungs-Verschlüsselung verwendet wurde, die Registrierung verloren.

LCOS-Änderungen 10.50.0145 Rel

Neue Features

→ Unterstützung von RADIUS Dynamic Peer Discovery nach RFC 7585

Korrekturen / Anpassungen

Allgemein

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

→ 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. (CVE-2021-33903)

→ 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.

VPN

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

→ Nach einem Abbau und anschließendem Neu-Aufbau einer VPN-Verbindung (sowohl IKEv1 als auch IKEv2) mit IPv6 auf einem vRouter oder LANCOM ISG-8000 wurden die VPN-Regeln (SA) nicht korrekt aufgebaut. Dadurch war keine Kommunikation über die VPN-Verbindung mehr möglich.

VoIP

→ 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.

→ 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.

→ 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 statt 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.
Die Übermittlung des zweiten Re-INVITEs der SIP-TK-Anlage wird jetzt erst übertragen, wenn die erste Aushandlung abgeschlossen ist.

LCOS-Änderungen 10.50.0129 RC3

Neue Features

Allgemein

→ Neuer DSL-Linecode für Geräte der LANCOM 1926-Serie
→ Auf den DSL-Routern der Serien 19xx und 179x kann zwischen dem aktuellem und einem alternativem DSL-Linecode umgeschaltet werden.
→ Unterstützung eines DNS-Filters zur Erkennung und Filterung von ungewünschten DNS-Datentunneln auf der Clientseite.
→ Unterstützung von IPv6 Prefix Discovery bei 464XLAT nach RFC 7050
→ Der WLC schaltet DNS-Server und DNS-Forwarder auf verwalteten APs ab.
→ Neuer VPN-Analyse-Befehl ‚ikectl' auf der Kommandozeile
→ Unterstützung von automatischer Path MTU Detection bei IPSec.

Korrekturen / Anpassungen

Allgemein

→ Im WEBconfig konnten nur die Benutzerdaten eines ausgewählten Public Spot-Benutzers ausgedruckt werden. Wenn mehrere Benutzerdatensätze zum Druck ausgewählt wurden, endete der Druckvorgang in einer endlosen Ladeschleife.
→ Ein Zugriff per LL2M auf ein Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „user unknown on remote system" quittiert.
→ Das Erstellen eines Wireshark-Trace per LCOSCap auf einem Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „cannot retrieve PSK" quittiert.

LCOS-Änderungen 10.50.0115 RC2

Neue Features

WLAN

→ Unterstützung für Fast Roaming over-the-DS

Korrekturen / Anpassungen

Allgemein

→ Nach einer Aktualisierung auf LCOS 10.50 RC1 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.

→ Es konnte in Einzelfällen vorkommen, dass Sessions nicht ordnungsgemäß abgebaut wurden (u.a. bei Verwendung von IPSec-over-HTTPS) und der reservierte Speicher nicht wieder freigegeben wurde. Dies führte dazu, dass weitere Pakete verworfen wurden und die Kommunikation nur noch stark eingeschränkt möglich war.

→ 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.

LCOS-Änderungen 10.50.0091 RC1

Neue Features

→ Performance-Optimierung durch Multicore-Unterstützung für LANCOM ISG-8000 bei IPsec-VPN
→ Unterstützung von Bidirectional Forwarding Detection (BFD) bei BGP
→ (Sub-Second-)Session-Switchover für Dynamic Path Selection (DPS)
→ DPS: ICMP-Messintervalle unterstützen nun Intervalle mit einer Zeitauflösung in Millisekunden
→ DPS: Neben ICMP wird auch HTTP(S) als Messmethode unterstützt
→ Unterstützung der CLAT-Seite von 464XLAT für IPv6-only im Mobilfunk
→ Unterstützung von NPTv6 (Präfix-NAT) bei IPv6
→ Der Loadbalancer unterstützt nun IPv6.
→ Unterstützung von IPv6-Leitungs-Polling
→ In der IPv6-Firewall können MAC-Adressen als Stationsobjekt (Quelle) konfiguriert werden.
→ In der IPv6-Firewall kann ein delegiertes Provider-Präfix als Stationsobjekt konfiguriert werden um ein dynamisches Präfix in einer Router-Kaskade freizugeben.
→ In Anwendungen, in denen DNS-Namen konfiguriert werden können, kann die bevorzugte Adressfamilie (IPv4 oder IPv6) angegeben werden.
→ Dynamic Path Selection (DPS) unterstützt nun IPv6.
→ Unterstützung für Curve448 im SSH
→ Der Public Spot unterstützt nun IPv6.
→ Public Spot: Das MAC-Adressformat ist nun konfigurierbar.
→ Unterstützung für RADIUS-Attribute nach RFC 5580
→ Der DHCP-Client zeigt nun die Lease-Time im Status-Menü an.
→ Die Rx / Tx Bandbreitenbegrenzung wird nun auch bei bei 802.1x-RADIUS-Authentifzierung ausgewertet.
→ Die Layer-7-Anwendungserkennung und DNS-Namen in der Firewall sind nun in einer gemeinsamen Tabelle zu konfigurieren.
→ Support von Session-Cookie und Anti-CSRF-Token in der WEBconfig.
→ Klartextpasswörter des Hauptgerätepasswords sind nach einem Gerätereset deaktiviert.
→ Die IKEv2-Lifetimes sind nach einem Gerätereset an die aktuellen BSI-Empfehlungen angepasst.
→ SHA-1 ist nach einem Gerätereset nicht mehr im IKEv2-Default-Proposal enthalten.

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.

→ Das delegierte IPv6-Provider Präfix kann über IKEv2-Routing an die VPN-Gegenstelle übermittelt werden.
→ Die Unterstützung für H.323 in der IPv4-Firewall entfällt.
→ Der vRouter unterstützt nun KVM als Hypervisor-Plattform.

Korrekturen / Anpassungen

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.
→ Bei Verwendung des SIP-ALG konnte es vorkommen, dass der Port für die RTP-Kommunikation ungültig wurde und ein eingehendes RTP-Paket mit der Meldung „ICMP Destination unreachable (Port unreachable)" abgelehnt wurde. Dies führte bei einem ausgehenden Telefonat zu einer einseitigen Sprachübertragung seitens des angerufenen Teilnehmers.
→ Der Voice Call Manager unterstützt mehrere Streams mit verschiedenen Codecs. Diese müssen aber während des Rufaufbaus initialisiert werden.
→ Wurde ein Anruf initial mit einem Stream aufgebaut (z.B. G.711) und im Re-INVITE ein zweiter Stream hinzugefügt (z.B. T.38), konnte der Voice Call Manager den zweiten Stream nicht verarbeiten. Dadurch wurden Daten-Pakete des zweiten Streams nicht weiter übertragen.