Release Notes

LCOS
10.72 RU7

Inhaltsübersicht

03 **1. Einleitung**

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

04 **3. Gerätespezifische Kompatibilität zu LCOS 10.72**

04 **4. Hinweise zu LCOS 10.72**
04 Informationen zu Werkseinstellungen
04 Entfall der VPN-Regeln in der IPv4-Firewall

05 **5. Feature-Übersicht LCOS 10.72**

05 **5.1 Feature-Highlights 10.72**
05 Advanced Mesh VPN

05 **5.2 Weitere Features LCOS 10.72**
05 Jugendschutz nach BPjM-Vorgaben
05 Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN

07 **6. Historie LCOS 10.72**
07 LCOS-Änderungen 10.72.0593 RU7
09 LCOS-Änderungen 10.72.0484 RU6
11 LCOS-Änderungen 10.72.0385 RU5
13 LCOS-Änderungen 10.72.0291 RU4
16 LCOS-Änderungen 10.72.0203 RU3
19 LCOS-Änderungen 10.72.0092 SU2

19 LCOS-Änderungen 10.72.0091 RU1
22 LCOS-Änderungen 10.72.0015 Rel

24 **7. Allgemeine Hinweise**
24 Haftungsausschluss
24 Sichern der aktuellen Konfiguration
24 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 10.72 RU7 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Updates 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 www.lancom.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 10.72

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
www.lancom.de/produkte/firmware/software-lifecycle-management

Die Unterstützung für die folgenden Geräte entfällt ab LCOS 10.72:

→ LANCOM 1781EF+
→ LANCOM 1783VA
→ LANCOM 1781VAW
→ LANCOM 1783VA-4G
→ LANCOM R883VAW
→ Business LAN R800A

4. Hinweise zu LCOS 10.72

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.

Entfall der VPN-Regeln in der IPv4-Firewall
Ab LCOS 10.70 werden VPN-Regeln zur Erzeugung von Netzbeziehungen (SAs) in der IPv4-Firewall nicht mehr unterstützt und durch die Konfigurationsmöglichkeit ‚Netzwerk-Regeln' im VPN-Menü ersetzt.
Dies betrifft hauptsächlich Szenarien mit IKEv1-Verbindungen.

Für weitere Details siehe:
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=85885720

5. Feature-Übersicht LCOS 10.72

5.1 Feature-Highlights 10.72

Advanced Mesh VPN

Bei klassischen, sternförmigen VPN-Standortvernetzungen, in denen alle Filialen lediglich über die Zentrale und nicht direkt untereinander verbunden sind, wird die Internetleitung der Zentrale schnell zum Flaschenhals der gesamten Kommunikation. Mit Advanced Mesh VPN kommunizieren die Zweigstellen nun auf direktem Weg miteinander und sorgen so in der Zentrale für deutlich weniger Traffic und einhergehend für höhere Performance. Die VPN-Tunnel werden hierbei bei Bedarf dynamisch aufgebaut, sobald Datentraffic von einer zur anderen Filiale transportiert wird. Findet keine Kommunikation mehr statt, wird die VPN-Verbindung ebenso dynamisch wieder abgebaut.

5.2 Weitere Features LCOS 10.72

Jugendschutz nach BPjM-Vorgaben

Mit LCOS 10.70 RC1 maximieren Sie jetzt den Schutz von minderjährigen Nutzern z. B. in Schulen oder Jugendeinrichtungen. So ist die offizielle Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) nun auch Teil der LANCOM Content Filter Option oder separat über die Software-Erweiterung LANCOM BPjM Filter Option erhältlich (ab LCOS 10.70 Rel). Damit sind Domains, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine stetige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet.

Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN

Immer dann, wenn ein hohes Sicherheitslevel für Ihre sensiblen Daten erforderlich ist oder z. B. auch Compliance-Richtlininen in Ihrem Unternehmen es vorsehen, ist die doppelte Absicherung des Netzwerk-Zugangs über den LANCOM Advanced VPN Client ideal. Dank Zwei-Faktor-Authentifizierung (IKEv2 EAP-OTP) schützen Sie jetzt den VPN-Zugang und damit auch Ihr Netzwerk vor unbefugten Zugriffen. So kann festgelegt werden, dass sich User ausschließlich über den LANCOM Advanced VPN Client einwählen können, sofern sie beim Login die Zwei-Faktor-Authentifizierung nutzen. Hierbei wird das VPN-Passwort um ein zeitbasiertes Einmalpasswort ergänzt, welches in einer Authentifizierungs-App (z.B. Google Authenticator) auf dem Mobiltelefon generiert werden kann.

Nutzbar ist dieses Feature mit allen Geräten, die mindestens 25 VPN-Tunnel besitzen (entweder bereits integriert oder aber mit LANCOM VPN Option aufgerüstet).

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

6. Historie LCOS 10.72

LCOS-Änderungen 10.72.0593 RU7

Korrekturen / Anpassungen

Allgemein

→ In einem Szenario mit DPS (Dynamic Path Selection) funktionierte auf zentralen Geräten ein Wechsel der Session auf eine bessere Leitung (passiver Switchover für DPS) für UDP-Pakete nicht.

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

→ Auf 5G-Routern mit IPv6-only-Mobilfunk-Verbindung wird neben dem IPv6-Kontext auch ein IPv4-Kontext aufgebaut. Der IPv4-Kontext meldet nach zwei Minuten wegen Inaktivität ein ‚Link-Down'. Dies führte fälschlicherweise dazu, dass die gesamte Mobilfunk-Verbindung abgebaut wurde.

→ In einem Szenario mit Config-Sync konnte es vorkommen, das aufgrund eines fehlgeschlagenen TLS-Handshakes 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.

→ Die ‚Layer 7-Anwendungserkennung' konnte Pakete mit QUIC nicht auflösen, wodurch entsprechender Datenverkehr nicht in der Statistik aufgeführt wurde.

→ Bei Verwendung des Browsers Safari unter iOS / macOS konnte die Konfiguration nicht per WEBconfig gespeichert werden.

→ 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.

→ Wenn bei einem Dual Stack Lite-Anschluss ein Wechsel des ‚Address Family Transition Router' (AFTR) des Providers durchgeführt wurde, konnte es vorkommen, dass die neue DNS-Adresse des AFTR nicht erreicht werden konnte, da aufgrund eines Problems mit dem DNS-Cache noch die DNS-Adresse des vorherigen AFTR verwendet wurde.

→ Bei sehr umfangreichen Konfigurationen konnte es in Verbindung mit sehr vielen, schnell aufeinander folgenden Zugriffen auf das Gerät (etwa per WEBconfig) beim Schreiben der Konfiguration per LANconfig in Einzelfällen vorkommen, dass das Gerät annahm, dass kein Haupt-Geräte-Passwort gesetzt war.

→ Sendet ein Internet-Provider bei Bezug der IPv6-Parameter per PPP kein ‚Router Advertisement', stellt der Router anschließend eine Anfrage per DHCPv6 mit IA_NA und IA_PD. Wenn in der DHCPv6 Advertise-Meldung vom Provider kein IA_NA enthalten war oder stattdessen die Meldung „NoAddrAvailable" ausgegeben wurde, konnte der Router kein IPv6-Präfix beziehen und die Kommunikation war nicht möglich.
In einem solchen Fall sendet der Router jetzt ein neues ‚Solicit' an den Provider, welches lediglich IA_PD enthält.

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.

→ In Einzelfällen konnte es zu einem unvermittelten Neustart des Routers kommen, wenn kurz hintereinander sehr viele VPN-Aushandlungen erfolgten.

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.

→ Leitete der Voice Call Manager ein eingehendes Telefonat an einen internen Benutzer mit Mehrfach-Anmeldung (SIP-Benutzer mit mehreren SIP-Registrierungen oder ISDN-Benutzer mit aktiviertem Parallelruf), welcher das Telefonat an einen weiteren Teilnehmer weiterleitete, sendete der Voice Call Manager keine Quell-Rufnummer. In der Folge wurde die Rufnummer des ursprünglichen Anrufers nicht an den weiteren Teilnehmer gesendet.

→ 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.

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

LCOS-Änderungen 10.72.0484 RU6

Korrekturen / Anpassungen

Allgemein

→ Wenn das entfernte Ziel (etwa ein Access Point) bei einem L2TP-Tunnel zu einem Router mehrere Pakete mit einem ACK bestätigte, führte dies dazu, dass die Sessions auf dem Router nach Verbindungsabbau nicht gelöscht wurden. Dadurch konnten die L2TP-Verbindungen nicht erneut aufgebaut werden.

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

→ Durch ein fehlerhaftes BGP-Basisattribut konnte es zum Abbruch der BGP-Verbindung kommen (VU#347067).

→ Waren auf einem Router mehrere ARF-Netzwerke mit der gleichen IP-Adresse konfiguriert (per VLAN separiert), wurde durch eine Konfigurations-Änderung 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.

→ Das IDS blockierte die Keepalive-Pakete eines GRE-Tunnels, da die Firewall in GRE-Paketen nach dem Protokollfeld mindestens 2 Byte an Nutzdaten erwartete. Dies führte dazu, dass der GRE-Tunnel immer wieder abgebaut wurde.

→ Wenn über eine PPTP-Verbindung so viele Daten übertragen wurden, dass die Übertragungs-Warteschlange vollief, obwohl die ‚Flow-Control' bereits Pakete verwarf, führte dies zu einem unvermittelten Neustart des Routers.

→ Ein GPON-Modul, welches bereits in einem LANCOM Router verwendet und erfolgreich mit einem Internetanschluss der Deutschen Telekom verbunden war, funktionierte in einem anderen LANCOM Router nicht mehr, obwohl es durch die Erstnutzung der OLT (Optical Line Termination) bereits bekannt war.

→ 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.

VPN

→ Empfing der Router bei aufgebauter IKEv2-Verbindung ein ‚Informational-Request' mit einer DELETE(CHILD_SA) Message, gefolgt von einer DELETE(IKE_SA) Message, führte dies zu einem unvermittelten Neustart des Routers.

WLAN

→ Der Quell-VLAN-Check (Setup / Public-Spot-Module / Check-Origin-VLAN) im Public Spot funktionierte nur für VLANs, welche per RADIUS zugewiesen wurden. Erfolgte die VLAN-Zuweisung über eine andere Methode (etwa per Circuit-ID), wurde der WLAN-Client nicht vom Public Spot abgemeldet und konnte in weiteren vorhandenen Public Spot SSIDs kommunizieren.

VoIP

→ Empfing der Voice Call Manager bei einem eingehenden Telefonat in einem Dialog (‚180 Ringing', ‚183 Session Progress' oder ‚200 OK') ein doppeltes ‚Connection Information' mit unterschiedlichen IP-Adressen, konnte es vorkommen, dass der Voice Call Manager die Antwort an die falsche IP-Adresse sendete. Dies führte zu einer einseitigen Sprachübertragung.

→ Nach einem Wechsel des SIP-Servers verblieb die IP-Adresse des alten Servers im Cache statt diese zu löschen. Dadurch hatte der Eintrag für den alten SIP-Server weiterhin die höchste Priorität, sodass kein Wechsel auf den neuen SIP-Server erfolgte. Wenn der alte SIP-Server nicht mehr funktionsfähig war oder die Registrierung ablehnte, führte dies dazu, dass keine Telefonie mehr möglich war.

→ Bei einem Anruf, welcher von einer ISDN-TK-Anlage am einen SIP-Teilnehmer weitergeleitet wurde, konnte es aufgrund eines falschen Transcoding-Vorgangs sporadisch zu einer einseitigen Sprachübertragung kommen.

LCOS-Änderungen 10.72.0385 RU5

Korrekturen / Anpassungen

Allgemein

→ Bei einem LANCOM 1793VA-4G blieb die SIM-Karte offline, wenn der Router stromlos war oder ein Kaltstart über die Kommandozeile durchgeführt wurde.

→ Ein neu hinzugefügter ‚Virtueller Link' wurde bei aktiviertem OSPF nicht automatisch erkannt. OSPF musste dazu global deaktiviert und wieder aktiviert werden.

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

→ Nach einer undefinierten Zeit (u.U. mehrere Wochen) schaltete sich das WWAN-Modul selbständig ab und war dann im Status ‚Deaktiviert'. 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.

→ Wenn ein SFP-GPON-1 Modul mit aktivierter ‚Dying Gasp'-Funktion in den LANCOM Router eingesteckt wurde, fand keine automatische Konfigurationsänderung mit nachfolgendem Neustart des Moduls statt. In der Folge startete die PON Management-Verbindung nicht und verblieb im Status ‚Opening management connection'.

→ Bei einigen LANCOM Routern fehlte in der Konfiguration die OID 1.2.20.10 (Pfad ‚Setup/LAN-Bridge/Protocol-Table' in der CLI / Menü ‚Schnittstellen / LAN / LAN-Bridge / Protokolle' in LANconfig & LMC).

→ Es konnte bei LANCOM Mobilfunk-Routern zu einem Fehlverhalten bei der Re-Initialisierung des USB-Moduls kommen, was zu einem unvermittelten Neustart des Routers führte.

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

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

→ Wenn in kurzer Zeit mehrere hundert oder tausend Meldungen im DNS gesendet wurden, konnte es vorkommen, dass dies mehr Speicher belegte als ursprünglich dafür reserviert wurde. Dies führte zu einem unvermittelten Neustart des Routers.

→ Bei Verwendung des 802.1X-Authenticators auf einem LAN-Port lernte der Router die MAC-Adresse eines angeschlossenen Gerätes, obwohl dieses nicht authentifiziert war. Dadurch war die Kommunikation mit dem verbundenen Gerät möglich.
MAC-Adressen werden nun bei Verwendung des 802.1X-Authenticators nicht mehr automatisch gelernt und die Kommunikation somit unterbunden.

→ Der TR-069-Dienst sendete seine Anfragen mit der IP-Adresse statt dem DNS-Namen des ACS-Servers. Dies führte bei einem strikt konfigurierten ACS-Server mit SNI dazu, dass die TLS-Verbindung abgebaut wurde, da die URI und der Name im Zertifikat nicht übereinstimmten.

VPN

→ Empfing ein LANCOM Router eine ‚INVALID_SPI Notification' von einem anderen Router, löschte der LANCOM Router die Child SA der zugehörigen IKEv2-Verbindung. Dabei konnte es vorkommen, dass der Speicher der gelöschten Child SA doppelt belegt wurde. Dies führte zu einem unvermittelten Neustart des Routers.

WLAN

→ In einem ‚Config Sync'-Szenario startete der Slave WLC unvermittelt neu, wenn vier oder mehr Einträge in eine Statustabelle über Fehler in der Konfiguration geschrieben wurden.

→ Wenn ein LANCOM Access Point via LMC verwaltet wurde und es eine SSID mit 802.1X (RADIUS)-Authentifizierung zu einem RADIUS-Server mit einem Namen, der länger als 15 Zeichen war, gab, konnte es vorkommen, dass ein falscher RADIUS-Server angesprochen wurde. Grund dafür war, dass es in der LMC keine Prüfung auf die Länge des RADIUS-Profil-Namens gab und das LCOS nur Namen mit maximal 15 Zeichen verwendete.

VoIP

→ Bei der DNS-Auflösung von SRV Records per NAPTR wurde in der Ausgabe des Konsolen-Befehls ‚show vcm dns' immer ein SRV Record mehr angezeigt als tatsächlich aufgelöst wurde.

→ Wenn der Router in einem SIP-Trunk-Szenario mit Gateway-Leitung zu einer SIP-Telefonanlage ein ‚RE-INVITE' vom SIP-Provider auf dem SIP-Trunk mit ‚refresher' im ‚Session-Expires'-Header (in diesem Fall ‚refresher=uas') empfing, änderte der Voice Call Manager den ‚refresher' im „200 OK" an den SIP-Provider (in ‚refresher=uac'), was nicht zulässig ist. Dies führte dazu, dass der Anruf vom SIP-Provider unterbrochen wurde.

LCOS-Änderungen 10.72.0291 RU4

Korrekturen / Anpassungen

Allgemein

→ Nach Aktivierung einer VPN-25-Option auf einem Router (kein Neustart erforderlich) konnte bei aktivierter CA das Geräte-Zertifikat in WEBconfig nicht über die Option ‚Aktuelles CA-Zertifikat herunterladen' heruntergeladen werden. Der Vorgang wurde mit der Fehlermeldung „Not Found" quittiert. Der Download des Zertifikats war erst nach einem Neustart möglich.

→ Bei einer seriellen Geräteverbindung wurde eine aktive Session nicht getrennt, wenn der Befehl ‚passwd -n' in einem Skript verwendet wurde.

→ Die Werteangabe zur Speicherauslastung wurde bei LANCOM Geräten mit LCOS falsch auf der Display-Seite ausgegeben.

→ Nach einer Änderung der LMC-Parameter durch die LMC (Setup/LMC) wurde die bisherige HTTPS-Session weiterverwendet. Wenn die Parameter fehlerhaft waren, führte dies dazu, dass das Gerät die LMC nach einem Neustart nicht mehr erreichen konnte.
Die HTTPS-Session wird jetzt nach Änderung der LMC-Parameter neu aufgebaut. Kann das Gerät die LMC mit den geänderten Parametern nicht mehr erreichen, erfolgt ein Rollback auf die bisherigen Parameter.

→ Üblicherweise verteilen Internet-Provider die Parameter eines IPv6-Anschlusses, indem initial ein Router-Advertisement gesendet wird. Wenn ein Internet-Provider stattdessen initial die IPv6-Parameter per DHCPv6 versendete und erst nach längerer Zeit ein Router-Advertisement mit dem Gateway, wurde das Gateway nicht in der Tabelle ‚Status/WAN/IP-Addresses/IPv6' angezeigt.
Nach einer Änderung des Gateways wird dieses jetzt in die Tabelle übernommen.

→ Bei einem Aufruf eines SNMP-Pfades in der MIB-2 wurden bei Routern der 1900-Serie die Informationen zum SFP-Port doppelt ausgelesen und der Speicher nicht wieder freigegeben. Dadurch konnte es bei immer wiederkehrendem Auslesen des SNMP-Pfades über einen längeren Zeitraum dazu kommen, dass kein freier Speicher mehr zur Verfügung stand. Dies führte zu einem unvermittelten Neustart des Routers.

→ Wenn bei Verwendung des ‚802.1X Authenticators für ETH-Ports' an einem Port mehr als eine MAC-Adresse erkannt wurde, führte dies dazu, dass der Port heruntergefahren wurde und somit keine Kommunikation mehr über diesen Port möglich war.
Im Konsolen-Pfad ‚Setup/LAN/IEEE802.1x/Authenticator-Ifc-Setup' gibt es jetzt die Option ‚Single-Host-Violation-Block'. Wird diese auf ‚No' gesetzt, kann nur das erste authentifizierte Gerät über den Port kommunizieren. Datenverkehr weiterer angeschlossener Geräte wird dann blockiert.

→ Wurde auf einem Router der 1900-Serie mit 5G-Modul der Befehl ‚Default' im Konsolen-Pfad ‚Setup/COM-Ports/WAN/Devices' ausgeführt, war die Tabelle anschließend leer. Dadurch wurde für das 5G-Modul implizit der Modus ‚Operating' auf ‚No' gesetzt, sodass das 5G-Modul deaktiviert war.
Wenn ein Gerät nicht in der Tabelle ‚Setup/COM-Ports/WAN/Devices' vorhanden ist, wird jetzt der Modus ‚Operating' auf ‚Yes' gesetzt.

→ Wenn ein LANCOM Router vom Auto Configuration Server (ACS) per TR-069 ein Leerlauf-Zeitfenster für eine Firmware-Aktualisierung erhielt (Modus ‚when idle'), wurde die Aktualisierung nicht durchgeführt, nachdem das Leerlauf-Zeitfenster endete.

→ Wurde bei einem Bezug der Konfiguration von einem Auto Configuration Server (ACS) der Telekom per TR-069 auch die Telefonie konfiguriert, trug der Router für den Registrar immer die URL ‚tel.t-online.de' ein, auch wenn diese nicht vom ACS übermittelt wurde.

→ EAPoL-Frames können jetzt per Mulicast übertragen werden, wenn im Menü ‚Setup/LAN/IEEE802.1x/Authenticator/IFC-Setup' die entsprechende Option aktiviert ist. Beim Multi-Host-Modus werden hierdurch Identity Requests für die RADIUS-Authentifizierung eines LANCOM Access Point per Multicast statt per Unicast gesendet.

→ In der Konfiguration eines LANCOM Routers war es möglich, eine logische WAN-Schnittstelle (z.B. DSL-1) für mehrere physikalische Schnittstellen (z.B. SFP-Port und ETH-Port) zu verwenden. In diesem Fall konnte es zu Problemen bei der (PPPoE)-Einwahl in WAN-Verbindungen kommen.

WLAN

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

VoIP

→ 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.

→ Wenn der LANCOM Router bei einem CompanyFlex-Anschluss als Session-Border-Controller (SBC) mit einer vorgeschalteten TK-Anlage eingesetzt wurde, funktionierte bei einer verschlüsselten Verbindung die DTMF In-Band-Übertragung nicht.

LCOS-Änderungen 10.72.0203 RU3

Korrekturen / Anpassungen

Allgemein

→ Bei einer Weiterleitung auf einen externen RADIUS-Server wurde beim LANCOM 1800EFW die angegebene IP-Adresse in umgekehrter Reihenfolge in die Konfiguration eingetragen.

→ Wird die Feature-Aktivierung per Konsole initiiert und der Lizenz-Server ist nicht erreichbar, verbleibt die Aktivierung im Zustand ‚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.

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

→ Der Zähler für das Datenvolumen-Budget berücksichtigte nicht die Daten, die über IPSec-Verbindungen übertragen wurden.

→ 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.

→ Im WEBconfig-Dashboard wurde in der Dienste-Übersicht für Web-Services der HTTPS-Port mit ‚1' statt ‚443' angezeigt.

→ 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.

→ Wenn zur Authentifizierung an einem LANCOM Router ein RADIUS-Server verwendet wurde und diese Authentifizierung nicht funktionierte, schlug das Fallback auf die lokale Authentifizierung fehl (Login blieb stehen), und der Router führte nach einigen Minuten einen unvermittelten Neustart durch.

→ Wenn bei einem Mobilfunk-Router mit 5G-Modul im laufenden Betrieb die SIM-Karte gewechselt wurde, führte dies zu einem unvermittelten Neustart.

→ War bei aktivierter DNS-Weiterleitung kein DNS-Server hinterlegt, meldete der Router dies nicht an den anfragenden Netzwerk-Teilnehmer.
Der Router sendet in einem solchen Fall jetzt die Meldung „server failure“ an den anfragenden Netzwerk-Teilnehmer.

→ Soll bei Verwendung der Funktion ‚Administrative Distanz‘ Portforwarding auch für die Verbindung mit dem höheren Wert (Backup-Verbindung) möglich sein, muss für diese ein weiterer Routing-Eintrag erstellt werden (Dummy-Route). Diese Dummy-Route wurde bei einem Portforwarding nicht berücksichtigt, sodass Pakete über die Backup-Verbindung nicht weitergeleitet werden konnten.

VPN

→ Wurde eine IKEv2-VPN-Verbindung auf AES-GCM konfiguriert, wurden eingehende, fragmentierte ESP-Pakete mit einer Fehlermeldung verworfen.

→ 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.

→ Bei Verwendung einer IKEv2-Verbindung per RAS Config Mode zwischen zwei LANCOM Routern mit aktiviertem IPv4-Routing wurden die hinterlegten Netzwerke zweimal übertragen. In einem VPN-Status-Trace wurde in diesem Fall die Meldung „IKEv2 Routes have been already exchanged“ ausgegeben. Dadurch kam es zu Fehlern auf der VPN-Verbindung.

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

→ 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.

→ Erhielt der Router vom SIP-Provider ein Re-INVITE mit SDP-Parametern, die

→ Bei einem Fehler des primären SIP-Servers erfolgt ein Wechsel auf einen SIP-Server mit niedriger Priorität. Dabei soll ein Wechsel zurück auf den primären SIP-Server erst nach 15 Minuten erfolgen. Bisher prüfte der Voice Call Manager bei jeder SRV-Auflösung, ob der SIP-Server mit der höchsten Priorität verwendet wurde und initiierte gegebenenfalls einen Wechsel. Weiterhin konnte es vorkommen, dass die Überprüfung des verwendeten SIP-Servers bereits während der Initialisierung durchgeführt wurde, wenn die IP-Adressen der SIP-Server noch nicht übermittelt waren.

→ Wenn ein am Router registriertes SIP-Telefon bei einem eingehenden Telefonat eine Anrufweiterschaltung durchführte und dabei direkt ein REFER mit anschließendem Re-INVITE sendete statt das Telefonat zu parken (Hold), führte dies dazu, dass vom SIP-Telefon zwei INVITE-Pakete für die gleiche Call-ID versendet wurden. Das Telefonat wurde daraufhin vom Provider abgebaut, sodass die Anrufweiterschaltung nicht möglich war.
Der Voice Call Manager verzichtet jetzt in einem solchen Fall auf die Authentifizierung bei dem Re-INVITE des SIP-Telefons und sendet dies direkt an das Weiterleitungs-Ziel. Das „SIP 200 OK“ vom Weiterleitungs-Ziel wird anschließend an das SIP-Telefon weitergeleitet, sodass das doppelte INVITE vermieden wird.

→ Erfolgte in einem Szenario mit einer ISDN-TK-Anlage eine Anrufweiterschaltung per FACILITY-Meldung und Call-Re-routing, wurde die Quellrufnummer nicht übernommen, wenn der Voice Call Manager kein SIP302 verwendete oder der SIP-Provider kein SIP302 unterstützte.

→ Bei einem eingehenden Telefonat an ein Analog- oder ISDN-Telefon berücksichtigte der Voice Call Manager bei der Auswahl des Codecs für den RTP-Datenverkehr nur die ursprüngliche SDP Offer anstelle der SDP-Answer. Dies konnte dazu führen, dass ein falscher Codec gewählt wurde. In einem solchen Fall war keine Sprachübertragung möglich und das Telefonat wurde nach kurzer Zeit abgebaut.
Der Voice Call Manager verwendet jetzt immer den Codec PCMA, sofern dieser im SDP Offer angeboten wird.

→ Wurde in einem Szenario mit einer ISDN-TK-Anlage ein ausgehendes Telefonat per Ziffernwahl initiiert, wurde die Rufnummer bei zu langsamer Übermittlung der einzelnen Ziffern durch die ISDN-TK-Anlage nicht komplett übertragen. Das Telefonat konnte dadurch nicht aufgebaut werden.
Der Voice Call Manager verwendet jetzt einen ‚Short Overlap Timer‘ von 500 statt 250 ms.

LCOS-Änderungen 10.72.0092 SU2

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 10.72.0091 RU1

Neue Features

→ Beim DHCPv6 Relay Agent können nun bis zu 4 Ziele zur Weiterleitungen an externe Server konfiguriert werden.

→ Der DHCPv6 Relay Agent unterstützt eine Absendeadresse in Richtung DHCPv6-Server.

→ Das BPJM-Modul besitzt nun eine CLI-Funktion zur Löschung der aktuellen Signaturdefinition.

→ „Connection Refused"-Meldungen werden nun im Syslog mit Level ‚Info' statt „Alarm" angezeigt. Dies führt dazu, dass diese Meldungen nicht mehr im Syslog der WEBconfig im Default angezeigt werden. Das Verhalten kann durch eine Konfigurationsänderung angepasst werden.

Hinweis:

Ab der nächsten LCOS-Major-Version werden die Spalten 'Tx-normal', 'Tx-reliable' und 'Tx-urgent' der Status-Tabelle 'Status/WAN/Packet-Transport' entfernt und nicht mehr unterstützt. Ebenso entfällt dort die Status-Tabelle Status/IP-Router/Protocol-Table. Die letzte unterstützte Version ist LCOS 10.7x.

Korrekturen / Anpassungen

Allgemein

→ Das Feature BPJM konnte auch konfiguriert werden, wenn keine Lizenz für diese Option vorhanden war.

→ Der WEBconfig-Setup-Assistent zur Einrichtung einer IPv6-Internetverbindung schrieb das Kommentarfeld in die ‚Router'-Spalte der IPv6-Routing-Tabelle. In der Folge war die konfigurierte IPv6-Verbindung nicht funktionsfähig.

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

→ 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 wieder in den Aktiv-Modus versetzt werden.

→ Wenn im Passwort einer verschlüsselten Konfigurationssicherung ein ‚+'-Zeichen enthalten war, konnte die verschlüsselte Konfigurationsicherung nicht mehr entschlüsselt und in das LANCOM Gerät übertragen werden.

→ 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 wiederhergestellt werden konnte.

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

→ 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.

→ 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.

→ Wenn bei einer DNS-Anfrage des LMC-Clients mehrere IP-Adressen aufgelöst wurden, verwendete das Gerät für die Kommunikation per TCP immer die ‚kleinste' IP-Adresse statt eine Lastverteilung auf mehrere IP-Adressen durchzuführen. Dieses Verhalten betraf auch weitere Anwendungen.
Es wird jetzt immer eine zufällige IP-Adresse verwendet.

VoIP

→ Wenn am Router Analog- bzw. ISDN-Geräte angebunden waren, sendete der Voice Call Manager im ‚SDP Answer' immer die Codecs PCMA (G.711-a) und PCMU (G.711-u), sobald einer der beiden Codecs im ‚SDP Offer' enthalten war. Jetzt werden alle Codecs außer PCMA und PCMU aus dem ‚SDP Offer' gelöscht und der erste Codec in die ‚SDP Answer' übernommen. Wenn PCMU verwendet wird, transcodiert der Voice Call Manager dies in PCMA, da ISDN- und Analog-Geräte lediglich PCMA unterstützen. Ist im INVITE kein ‚SDP Offer' enthalten, antwortet der Voice Call Manager im ‚SDP-Answer' mit PCMA und PCMU.

→ War in einer SIP-Leitung bei der ‚Signalisierungs-Verschlüsselung' die Option ‚Automatisch' ausgewählt (NAPTR aktiv), konnte es vorkommen, dass die Re-Registrierung nicht funktionierte und eine Neu-Registrierung durchgeführt werden musste. Dadurch funktionierte in diesem Zeitraum die Telefonie nicht mehr.

→ 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.

→ Verwendete ein SIP-Provider DNS-SRV-Einträge mit der gleichen Priorität, wechselte der Voice Call Manager bei jeder erneuten DNS-Auflösung zwischen diesen Servern. Dies führte zu einer kurzen Unterbrechung der Registrierung.

LCOS-Änderungen 10.72.0015 Rel

Neue Features

→ Unterstützung von Q-in-Q-VLAN auf WAN-Schnittstellen
→ Unterstützung einer Absendeadresse für den Updateprozess der Signaturdatei beim BPJM-Filter
→ Master-Holddown-Zeit-Schalter im VRRP
→ Unterstützung für RADSEC-Zertifikate im SCEP-Client
→ In der WEBConfig gibt es im Dashboard bei WLAN einer Verlinkung zur WLAN-Stationstabelle.
→ Ein LANCOM WLC unterstützt die Auswahl des LX-6500 im Firmware-Management.
→ Unterstützung von LANCOM ARC 2.0 zusammen mit der LMC

Korrekturen / Anpassungen

Allgemein

→ Obwohl auf einem Router keine Content Filter-Option aktiv war, wurde im WEBconfig das Menü ‚Content Filter' angezeigt. Die Konfigurationsdialoge waren jedoch leer.
→ In der WEBconfig fehlten im Menü ‚Datum/Zeit / Synchronisierung' die Konfigurationseinstellungen zur Zeitserver-Abgleichmethode.
→ Im WEBconfig-Menü 'Setup Assistent / Public Spot Benutzer verwalten' wurden Benutzer als ‚unauthenticated' angezeigt, obwohl diese erfolgreich mit dem Public Spot verbunden waren.
→ Bei einer WWAN-Verbindung, bei welcher der Adressbezug per DHCP konfiguriert war, sendete der LANCOM DHCP-Client ARP requests, obwohl diese für die WWAN-Verbindung nicht benötigt wurden.
→ Die in dem Menü ‚IPv4 / Adressen' hinterlegten DNS-Server sind an das LAN-Interface gebunden. Wenn in diesem Menü die lokale IP-Adresse des Routers als DNS-Server hinterlegt und eine Default-Route erstellt wurde, welche auf die IP-Adresse eines vorgeschalteten Routers im selben IP-Adress-Bereich zeigte, führte dies zu einem unvermittelten Neustart des Routers.

WLAN

→ Wenn bei voll ausgefüllter RADIUS-Benutzertabelle ein weiterer Benutzer hinzugefügt werden sollte, wurde anstatt einer Fehlermeldung eine Seite mit JavaScript-Code angezeigt.

→ In LCOS 10.70 konnte es vorkommen, dass in der Adress-Tabelle des verwendeten WLC-Tunnels ein fehlerhafter Verweis auf die MAC-Adresse des verbundenen WLAN-Gerätes hinterlegt wurde. Dadurch funktionierte die Kommunikation über den WLC-Tunnel nicht mehr.

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
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de