Release Notes

LCOS
10.80 RU10

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 10.80 RU10 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 10.80

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

LANCOM Geräte ohne Unterstützung ab LCOS 10.80

→ LANCOM LN-1700
→ LANCOM LN-1702
→ LANCOM LN-830acn
→ LANCOM L-822acn
→ WLC-4006+

4. Hinweise zu LCOS 10.80

Änderung des Attributs für E-Mail-Adressen bei der Verwendung von Zertifikaten

Ab LCOS 10.80 wird die das Attribut ‚E' für E-Mail-Adressen bei der Verwendung von Zertifikaten (z.B. für IKEv2) nicht mehr unterstützt. Stattdessen muss das Attribut ‚emailAddress' verwendet werden. Diese Änderung muss **vor** dem Update auf LCOS 10.80 durchgeführt werden.

Beispiel:
„/E=test@lancom.de" muss in „/emailAddress=test@lancom.de" geändert werden.

Weitere Informationen enthält der KB-Artikel https://support.lancom-systems.com/knowledge/display/KB/Konfiguration+einer+zertifikatsbasierten+IKEv2+VPN-Verbindung+zwischen+zwei+LANCOM+Routern.

Wichtige Hinweise zur Erweiterung der Eingabelänge des Hauptgeräte-passworts

Ab LCOS 10.80 wurde die Eingabemöglichkeit der Anzahl der möglichen Zeichen des Hauptgerätepassworts sowie der weiteren Administratoren von 16 auf 128 Zeichen erweitert. Sollten mehr als 16 Zeichen in LCOS 10.80 verwendet werden, so ist ein Downgrade auf Versionen kleiner als 10.80 nicht mehr möglich bzw. wird nicht unterstützt. Eine Anmeldung an einem Gerät ist nach dem Downgrade nicht mehr möglich.

Besondere Beachtung gilt dem WLC mit verwalteten Access Points im Falle der Passwortsynchronisierung. Sollte hier das längere Passwort auf dem WLC verwendet werden, so müssen alle verwalteten Access Points ebenfalls auf LCOS 10.80 betrieben werden. Eine lokale Anmeldung ist in diesem Fall auf APs mit LCOS kleiner 10.80 nicht mehr möglich.

Die oben genannten Hinweise gelten nur in dem Fall, falls die neue Möglichkeit von mehr als 16 Zeichen beim Passwort verwendet wird.

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 10.80

5.1 Feature-Highlight 10.80

Let‘s Encrypt für WEBconfig und den LANCOM Public Spot
Let‘s Encrypt ist eine Zertifizierungsstelle, die kostenlose HTTPS-Zertifikate anbietet, um verschlüsselte Verbindungen zu standardisieren. WEBconfig und auch der LANCOM Public Spot unterstützen nun Let‘s Encrypt. So lassen sich mit wenigen einmaligen und einfachen Handgriffen kostenlose und vertrauenswürdige Zertifikate erstellen, über das Gateway einbinden und automatisch verlängern.

5.2 Weitere Features LCOS 10.80

Zero-touch Rollout für Mobilfunk-Router
Mit der Unterstützung von Zero-touch ist die Einrichtung von LANCOM Mobilfunk-Routern nun noch einfacher und schneller. Wo zuvor eine manuelle Konfiguration des Mobilfunk-Zugangspunktes erforderlich war, genügt nun das Einsetzen einer PIN-freien SIM-Karte in das Gerät. Zero-touch Rollout ermöglicht eine automatische Verbindung mit dem Internet und darauf folgend mit der LANCOM Management Cloud, um die passende Konfiguration des Gateways abzurufen.

LANCOM vRouter über Google Cloud verfügbar
Mit LCOS 10.80 betreiben Sie den LANCOM vRouter auf Wunsch nun auch mit dem Cloud-Computing-Anbieter Google Cloud. So können Sie neben Microsoft Azure, VMware ESXi, Hyper-V und AWS nun auch Google Cloud nutzen, um die eigene Infrastruktur in die Cloud zu verlagern. Der LANCOM vRouter garantiert dabei die sichere Anbindung und übernimmt die verschlüsselte Kommunikation zwischen Ihrem Standort und Ihrer virtualisierten Infrastruktur in der Google Cloud. Darüber hinaus ist auch die Virtualisierung von Zentralen möglich: der vRouter in der Google Cloud ersetzt ganz einfach das zentralseitige Hardware-Gateway.

WEBconfig im neuen Corporate Design

Managen Sie Ihre Geräte über den Webbrowser, stellt LANCOM Ihnen über WEBconfig eine grafische Benutzeroberfläche bereit, die direkt in das LCOS integriert ist und ab sofort mit neuem Anstrich im modernen Design und maximaler Übersichtlichkeit glänzt.

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

6. Historie LCOS 10.80

LCOS-Änderungen 10.80.0966 RU10

Neue Features

→ In der Tabelle ‚WAN MTU-Liste' können nun bei Gegenstellen auch Wildcards verwendet werden.

Korrekturen / Anpassungen

Allgemein

→ Bei Aufruf der Aktionen ‚Delete-History' und ‚Retrain' per WEBconfig (Menü-Pfad ‚Extras / LCOS-Menübaum / Status / xDSL / xDSLx') wurde das Untermenü zum Ausführen der Befehle nicht geladen und stattdessen die Fehlermeldung „Not Found" ausgegeben.

→ War IPv6 auf einem Router aktiv, konnte es zu einem unvermittelten Neustart des Routers kommen, wenn Netflow eine FTP-Daten-Session analysierte, welche über IPv6 übertragen wurde.

→ Wenn in der Kommandozeile der Befehl „find vrrp" eingegeben wurde, enthielten die ausgegebenen Pfad-Informationen keine Zeilenumbrüche.

→ Waren bei einer VPN-Loadbalancer-Konfiguration als IPv4/IPv6-Zieladressen DNS-Adressen statt IP-Adressen angegeben, füllte sich die Tabelle im Pfad ‚Status/VPN/Load-Balancer/Peer-Status/' mit unendlich vielen Einträgen.

→ Auf Mobilfunk-Routern mit Quectel 4G- und 5G-Modulen wurde bei der Berechnung der Signalwerte RSRP (Reference Signals Received Power) und RSRQ (Reference Signal Received Quality) das Feld für den RSRP übersprungen. Dies führte dazu, dass für den RSRP und den RSRQ fehlerhafte und teils auch physikalisch unmögliche Werte ausgegeben wurden.
Die folgenden Mobilfunk-Router waren von dem Verhalten betroffen:

- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

→ Eine Plain-Ethernet-Gegenstelle mit dynamisch erzeugter MAC-Adresse (‚MAC-Adress-Typ' auf ‚Lokal') eines in Hyper-V betriebenen vRouters wurde nicht aufgebaut, sodass die Internet-Verbindung nicht zustande kam. Weiterhin konnten in einem solchen Szenario mehrere im vRouter angelegte Plain-Ethernet-Gegenstellen mit dynamischer MAC-Adresse untereinander keine ICMP-Pakete (Ping) austauschen.

→ Bei Mobilfunk-Routern mit Quectel 4G- und 5G-Modulen wurde die Provider-Bezeichnung im Status-Feld ‚Network' (Konsolen-Pfad ‚Status/Modem-Mobile/') auf 16 Zeichen begrenzt. Dadurch konnte es vorkommen, dass die Bezeichnung abgeschnitten wurde.
Die folgenden LANCOM Mobilfunk-Router waren von dem Verhalten betroffen:
- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

→ Nach einem Firmware-Update von durch die LMC verwalteten LANCOM L-322agn (Hardware Rev. 2) konnte es zu einem unvermittelten Neustart aufgrund von Speichermangel kommen.

→ Die Tabelle für die Auflistung offener Dienste im Pfad ‚Status/Config/Services' zeigte falsche Werte an.

→ Aufgrund zweier Sicherheitslücken wurde OpenSSL auf die Version 3.0.16 aktualisiert (siehe auch CVE-2024-13176 & CVE-2024-9143).

→ Bei mehrfachen Änderungen der Route zum BGP-Neighbor auf ein anderes Interface konnte es vorkommen, dass der Router versuchte, die BGP-Verbindung über ein falsches Interface aufzubauen. Dadurch kam die BGP-Verbindung nicht zustande.

→ Wenn sich die WAN-IP-Adresse des LANCOM Routers änderte (z.B. nach einer Zwangstrennung durch den Provider) wurden vorhandene Firewall-Sessions nicht entfernt. In der Folge wurde die veraltete WAN-IP-Adresse weiterhin verwendet, was dazu führte, das vorhandene VPN-Verbindungen nicht mehr genutzt werden konnten. Erst nach einem Neustart des LANCOM Routers wurde die aktuelle WAN-IP-Adresse verwendet und das Fehlverhalten damit behoben.

→ Der LANCOM 1930EF verfügt über sechs Ethernet-Schnittstellen, aber nur über vier virtuelle LAN-Interfaces. Da in LANconfig und in der LMC für dieses Gerät sechs LAN-Interfaces vorhanden waren, führte dies dazu, dass die Konfiguration per LANconfig und per LMC nicht auf den Router geschrieben bzw. ausgerollt werden konnte.
Es stehen jetzt sechs virtuelle LAN-Interfaces zur Verfügung.

→ Bei Verwendung des vRouters in Proxmox konnte es vorkommen, dass für den zugewiesenen RAM ein falscher Wert angezeigt wurde.

→ Wird eine Default-Route mit einer Internet-Verbindung unmaskiert betrieben, ist der DNS-Server aus dem WAN erreichbar. In der Dienste-Tabelle ‚Status/Config/Services' wurde aber nur die Default-Route mit dem Tag 0 berücksichtigt, sodass für unmaskierte Default-Routen mit einem von 0 abweichenden Routing-Tag fälschlicherweise der Status ‚No' angezeigt wurde.

→ Änderte man die Zuweisung des PON-Moduls z.B. von ‚LAN-1' nach ‚DSL-1', verblieb das PON-Management im Status ‚Working'. Dies konnte erst durch einen Neustart des Routers aufgelöst werden.

→ Empfing der Router ein ARP-Paket für ein ungültiges LAN-Interface (etwa bei einer fehlerhaften Konfiguration mit einer DNS-Weiterleitung an die eigene IP-Adresse), führte dies zu einem unvermittelten Neustart des Routers. In einem solchen Szenario wird der Eintrag im ARP-Cache ungültig und das Paket somit verworfen.

→ Bei Verwendung von XLAT mit Maskierung wurden eingebettete ICMP-Header nicht durch das XLAT maskiert. Da die Absende- und Ziel-Adresse dadurch gleich waren, wurden die Pakete durch die IDS-Erkennung blockiert.

VPN

→ Wenn eine VPN-Verbindung mit gleicher Namensbezeichnung sowohl als IKEv1-, als auch als IKEv2-Verbindung angelegt war, konnte es beim Zurückschreiben einer Konfiguration dazu kommen, dass der Router unvermittelt neu startete.

WLAN

→ Der Mechanismus zum Aufräumen der WLAN-ARP-Tabelle funktionierte nicht korrekt, wodurch es vorkommen konnte, dass Einträge für WLAN-Clients mehrfach vorhanden waren. Dies führte dazu, dass ARP-Pakete für diese WLAN-Clients nicht weitergeleitet wurden und somit die Kommunikation stark eingeschränkt war.

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.

LCOS-Änderungen 10.80.0833 RU9

Korrekturen / Anpassungen

Allgemein

→ Das LANCOM SFP-GPON-1 Modul wurde vom LANCOM 1930EF nicht erkannt. Der Status des Moduls verblieb im Konsolen-Pfad „Status/PON“ bei „Module in Waiting“.

→ 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.

→ Nachdem bei einem IPv6-Interface mit statisch konfigurierten Delegierungs-Adressen das IPv6-Interface deaktiviert und die Delegierungs-Adressen gelöscht wurden, waren die Delegierungs-Adressen nach Aktivierung des IPv6-Interfaces weiterhin vorhanden.

→ Ein IPv6-Interface soll nur dann nicht aufgebaut werden, wenn die DAD (IPv6 Duplicate Address Detection) bei der primären Link-Local-Adresse nicht erfolgreich ist. Das IPv6-Interface wurde aber auch dann nicht aufgebaut, wenn die DAD bei einer statisch vergebenen IPv6-Adresse, die vor der primären Link-Local-Adresse geprüft wurde, nicht erfolgreich war.

→ Im WEBconfig-Dashboard eines LANCOM vRouters wurden aktivierte Demo-Lizenzen nicht angezeigt.

→ Ein Ethernet-Interface wurde vom BGP nur dann auf Zustands-Änderungen überwacht, wenn die Verbindung zum BGP-Neighbor erfolgreich aufgebaut wurde. Wenn das Ethernet-Interface noch nicht erfolgreich aufgebaut war (etwa nach einem Neustart des Routers), bevor der Router versuchte die Quell-Adresse für den BGP-Neighbor aufzulösen, konnte die BGP-Verbindung nicht aufgebaut werden.
In einem solchen Fall wird jetzt eine Zustands-Überwachung gestartet, damit das BGP Änderungen am Interface erkennt.

→ Nach einem Hardware-Reset eines durch die LMC verwalteten R883+ oder R903 wurde das LMC-Zertifikat nicht gelöscht.

→ Wenn der LMC-Client eines Gerätes nach einem Rollout auf Daten von der LMC wartete, aber keine mehr ankamen (etwa aufgrund von Verbindungs-Problemen), führte dies zu einem unvermittelten Neustart des Gerätes.
→ Wenn in der Portforwarding-Tabelle mehr als 32 Einträge vorhanden waren, führte dies beim Schreiben der Konfiguration per LANconfig zu einem unvermittelten Neustart des Gerätes.
→ Wurde auf einem Mobilfunk-Router mit aktiver Mobilfunk-Verbindung die SIM-Karte getauscht, konnte das Mobilfunk-Modul anschließend keine Verbindung mehr aufbauen.
→ Bei Einsetzen einer nicht aktivierten SIM-Karte wurde statt der Fehler-Meldung „Limited Service“ der Fehler-Code 10 auf der Konsole (Mode) und im LANmonitor (Modus) angezeigt.
→ Wenn auf einem Router mit konfigurierter Backup-Verbindung nach dem Backup-Fall wieder auf die Haupt-Verbindung geschwenkt wurde, konnte es vorkommen, dass Datenverkehr eines nachgeschalteten Routers weiterhin über die Backup-Verbindung geleitet wurde und die Daten somit nicht übertragen werden konnten.
→ Trafen SMS-Pakete auf einem Mobilfunk-Router in einer falschen Reihenfolge ein, konnten die Trigger nicht korrekt durch die Aktions-Tabelle verarbeitet werden. Dies führte dazu, dass die hinterlegte Aktion nicht ausgeführt werden konnte (z.B. Nachbuchen von Datenvolumen).

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.
→ Bei Verwendung des Loadbalancers konnte es nach dem Abbau einer VPN-Verbindung in Einzelfällen vorkommen, dass die Verbindung nicht automatisch durch das Keepalive (Haltezeit 9999) aufgebaut wurde.

LCOS-Änderungen 10.80.0742 SU8

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 10.80.0741 RU7

Neue Features

→ Bei Verwendung des LANCOM SFP-GPON-1-Moduls an Gigabit-Anschlüssen der Deutschen Telekom wird vom BNG die erreichbare Datenrate auf 1,1 GBit/s gesetzt. Dies konnte dazu führen, dass die Download-Performance z. B. bei Internet-Speedtests aufgrund von Bursts statt bei ca. 930 MBit/s nur zwischen 700 und 800 MBit/s lag. Die Buffer im GPON-Modul wurden vergrößert und werden nun vom LCOS entsprechend für diesen Fall angepasst. Nach dem LCOS-Update wird diese Einstellung automatisch aktiviert. Auf der CLI ist das Verhalten schaltbar. In bestimmten Fällen kann es notwendig sein, dass die neuen Einstellungen erst nach einem erneuten LCOS-Neustart wirksam werden, nachdem die Internet-Verbindung erfolgreich aufgebaut wurde.

→ Nach einem Geräte-Reset ist der SFP-Port der LANCOM 1800EF-Serie nun als WAN-Port statt LAN-Port vordefiniert. Dies ermöglicht auch eine Zero-Touch-Inbetriebnahme an Glasfaseranschlüssen per SFP.

Korrekturen / Anpassungen

Allgemein

→ Im WEBconfig-Dashboard eines LANCOM vRouters wurden aktivierte Demo-Lizenzen nicht angezeigt.

→ Nach einer Zwangstrennung der WAN-Verbindung durch den ISP konnte es vorkommen, dass BGP im Status IDLE verblieb und nicht mehr arbeitete.

→ In der Konfiguration eines RADIUS-Servers war es nicht möglich, einen vorhandenen Backup-Server in einem Profil zu nutzen. Nach dem Speichern des Profils war die Auswahl nicht mehr vorhanden.

→ Es konnte vorkommen, dass der CRL-Client für einen kurzen Zeitraum keine CRL hatte, da diese bereits abgelaufen war und noch keine neue CRL bezogen wurde.

→ War die Verbindung zu einem BGP Neighbor beim Start von BGP nicht möglich, wurde die BGP-Verbindung nicht aufgebaut, nachdem der BGP Neighbor wieder erreichbar war. Dadurch war keine Kommunikation mit dem betroffenen BGP Neighbor möglich.

→ Wenn das Ziel-Interface zu einem BGP Neighbor im Status ‚down' war, versuchte der Router die Verbindung trotzdem aufzubauen und wechselte in den Status ‚active' bzw. ‚connect'.

→ Bei einem Import der *.ova-Datei eines vRouters in VMWare besteht die Möglichkeit, die IP-Adresse sowie die Subnetzmaske für ein Netzwerk über ein Feld in VMWare zu setzen. Dabei sollten die IP-Adresse und die Subnetzmaske durch ein Leerzeichen voneinander getrennt werden. Ein Leerzeichen war aber nicht erlaubt und konnte daher nicht eingegeben werden. Dies führte dazu, dass die Angabe der IP-Parameter in VMWare nicht möglich war
Die IP-Adresse und die Subnetzmaske können jetzt über ein Komma (,) voneinander getrennt werden.

→ Nach dem Löschen der ACS-URL durch einen ACS (Auto Configuration Server) per TR-069 antwortete der Router fälschlicherweise weiterhin auf Anfragen per TR-069 und versuchte weiterhin den ACS zu kontaktieren.

→ In Einzelfällen konnte es bei der Aktivierung / Deaktivierung des VPN-Moduls zu einem unvermittelten Neustart des Routers kommen, wenn währenddessen viele Firewall-Sessions auf- oder abgebaut wurden.

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.

→ In der RADIUS-Tabelle eines LANCOM WLC-60 konnten nur maximal 128 Einträge für Public Spot-Benutzer angelegt werden. Es sind jetzt maximal 256 Einträge möglich.

VoIP

→ Bei einem Ausfall aller TCP SIP-Server, die über NAPTR aufgelöst wurden, sendete der Voice-Call-Manager mehrere neue TCP-SYN-Pakete pro Sekunde zu allen Servern. Bei einem Ausfall aller UDP SIP-Server, die über NAPTR aufgelöst wurden, sendete der Voice-Call-Manager in einem festgelegten Zeitraum zu viele neue REGISTER-Pakete. Bei einer Nicht-Erreichbarkeit wird nun durch ein sog. Exponential Backoff eine fehlgeschlagene Anfrage in regelmäßigen Abständen mit zunehmender Verzögerung zwischen den Anfragen erneut durchgeführt.

→ In Szenarien, in denen der gleiche SIP-Server für die Registrierung via UDP, TCP und TLS verwendet wurde, priorisierte der Voice-Call-Manager die NAPTR-Records falsch, wenn der Empfang der DNS-Antworten eine andere Reihenfolge hatte als die gesendeten DNS-Antworten.

LCOS-Änderungen 10.80.0665 RU6

Neue Features

→ Bei Auslieferung ab Werk oder nach einem Konfigurationsreset mit LCOS 10.80.0664 PR ist eine neue Default-Gegenstelle mit dem Namen ‚GPON-Default' für Telekom-Glasfaseranschlüsse vorhanden, die eine Zero-Touch-Inbetriebnahme mit der LMC ermöglicht und automatisch am WAN- / SFP-Port (geräteabhängig) eine Telekom-PPPoE-Verbindung aufbaut. Diese Gegenstelle ist in allen Geräten der 1800EF-x-Serie, 180xVA-Serie und 19xx-Serie vorhanden.

→ Für IPv4-Firewall-Sessions wurde ein neuer Konfigurationsparameter eingeführt, mit dem die Anzahl der gelichzeitigen Firewall-Sessions limitiert werden kann. Im Default ist der Parameter ‚0', d.h. nicht limitiert. Der Parameter muss individuell für das Szenario manuell gesetzt werden.

→ Es wurden zusätzlich Counter für Überwachung der Anzahl von IPv4-Firewall-Sessions eingeführt.

Korrekturen / Anpassungen

Allgemein

→ In Szenarien mit mehreren WAN-Verbindungen verwendete der DNS-Dienst bei aktivem DPS standardmäßig die Leitung, welche mit ‚MOST_USED' klassifiziert wurde. Dies führte dazu, das DNS-Anfragen bei einer schlechten Internet-Verbindung nicht beantwortet wurden. Es wird nun standardmäßig wieder das Verfahren ‚ROUND_ROBIN' verwendet.

→ Bei der Installation eines vRouters mit LCOS 10.80 auf Hyper-V fror die Installations-Routine ein. Dadurch konnte die Installation nicht abgeschlossen werden.

→ Netflow belegte auch dann CPU-Ressourcen, wenn Netflow deaktiviert war.

→ Wenn Netflow sehr viele Sessions aufräumen musste, konnte es vorkommen, dass der Job zu lange brauchte. Dies führte zu einem unvermittelten Neustart des Routers.

→ Wurde an einen Router der LANCOM 1800EF-Serie, an den LANCOM 1650E oder an den LANCOM WLC-60 ein USB-Stick angeschlossen, konnte es vorkommen, dass dieser nicht korrekt erkannt wurde. Dies führte zu einem unvermittelten Neustart des Gerätes. Ebenso konnte es vorkommen, dass der unvermittelte Neustart bei gestecktem USB-Stick beim Auslesen des Konsolen-Pfades ‚Status/USB/Devices' auftrat.

→ Bei den LANCOM Geräten ISG-5000 / ISG-8000 sowie WLC-2000 wurden die Meta-Informationen für die LMC nicht bootpersistent gespeichert. Dadurch wurden bei Verwendung von Dynamic Path Selection die Informationen im LMC-Monitoring nicht korrekt angezeigt.

→ In Einzelfällen konnte es vorkommen, dass konfigurierte BGP-Neighbors doppelt erstellt wurden. Die erste Verbindung verblieb dabei dauerhaft im Status ‚Established'. Der Router versuchte aber immer wieder auch die zweite Verbindung aufzubauen, was zu einer Kollision mit der bestehenden Verbindung und damit zu einem Abbau der Verbindung führte. Dies wurde durch die Fehlermeldung „Connection collision resolution" quittiert.

→ Versuchte ein SSH-Client eine Verbindung zu einem Access Point oder Router mit dem veralteten und unsicheren Verschlüsselungs-Algorithmus ‚arcfour128' aufzubauen, führte dies zu einem unvermittelten Neustart des Gerätes.

VPN

→ In Szenarien mit mehreren VPN-Loadbalancern (etwa mit Dynamic Path Selection) wurden die VPN-Lizenzen nicht korrekt gezählt. Dies führte bei korrekter Lizenzierung dazu, dass in einem solchen Szenario zu wenig VPN-Lizenzen vorhanden waren und somit nicht alle VPN-Tunnel aufgebaut werden konnten.

→ Der Parameter ‚Remote-Auth' kann für IKEv2 im Konsolen-Pfad ‚Setup/VPN/IKEv2/Auth/Parameter/<VPN-Name>' nur dann auf EAP gesetzt werden, wenn mindestens 25 VPN-Lizenzen auf dem Router vorhanden sind (Central Site Gateway, Router der 19xx-Serie oder Router mit VPN-25 Option). Es wurde aber keine Fehlermeldung ausgegeben, sodass die Ursache nicht direkt ersichtlich war.
In einem solchen Fall wird jetzt die Fehlermeldung „Missing EAP license." ausgegeben.

→ Bei Verwendung eines IKEv2-Loadbalancers konnte es bei Überschneidung eines Auf- und Abbaus vorkommen, dass der Loadbalancer nicht mehr aufgebaut wurde.
Weiterhin wurden Sessions bei einem Wechsel auf ein anderes Interface nicht aus der Statistik gelöscht, sodass die Anzahl der Sessions fehlerhaft angezeigt wurde.

LCOS-Änderungen 10.80.0594 RU5

Neue Features

→ Bei Multicore-Geräten wird im Status-Menü bzw. als SNMP-OID nun auch die CPU-Auslastung von mehreren CPU-Kernen angezeigt.

→ Für RADIUS-Szenarien wurde ein neuer Schalter in mehreren Modulen eingeführt, der definiert, ob das Vorhandensein des ‚Message Authenticator-Attributs' in RADIUS-Nachrichten auf der Client-Seite (also die Seite, die ein ‚RADIUS-Accept /-Fail' empfängt) erzwungen wird.

→ Der 802.1X-Authenticator im LCOS akzeptiert keine Antworten ohne EAP-Message mehr.

→ Für Dynamic Path Selection / Loadbalancer-Szenarien wurde ein neuer Parameter hinzugefügt, der Sessions auf den am stärksten genutzten Kanal legt.

→ Im TR-069 kann konfiguriert werden, welche WAN-Verbindungen nicht vom TR-069-Client für die Verbindung zum ACS verwendet werden sollen.

→ Die Performance bei Anzeige der IPv4-Firewall-Verbindungliste bei großen Tabellen wurde verbessert.

→ Stabilitätsverbesserung bei der Ausgabe bzw. Anzeige der IPv4-Router-Verbindungsliste und Offene-Port-Liste in Szenarien mit sehr vielen Einträgen unter hoher Last.

→ Performance-Verbesserung beim automatischen Bereinigen der IPv4-Router-Verbindungsliste in Szenarien mit sehr vielen Einträgen.

→ Stabilitätsverbesserungen und Optimierungen im ARP, insbesondere in Szenarien unter Last.

Korrekturen / Anpassungen

Allgemein

→ Die SFP+-Schnittstellen eines LANCOM ISG-5000 bzw. ISG-8000 konnten nicht fest auf ‚10 GBit/s Fiber' eingestellt werden. Beim Zurückschreiben wurde eine Fehlermeldung ausgegeben.

→ Bei Verwendung der Accounting-Funktion konnte es vorkommen, dass der LANCOM Router während eines Firmware-Updates einen unvermittelten Neustart durchführte.

→ Bei Verwendung von VRRP auf Routern der 1800er-Serie (außer 1800EF, 1800EFW und 1800EF-5G) konnte die VRRP-Adresse nur dann angesprochen werden, wenn dem verwendeten Ethernet-Port eine Bridge-Gruppe statt einem LAN-Interface zugeordnet war.

→ In Einzelfällen konnte es bei Routern mit Multicore-CPU dazu kommen, dass der Scheduler dem TCP-Job keine Arbeit zuwies. Dadurch waren SSH-Verbindungen zum betroffenen Router sehr langsam und durch die LMC verwaltete Router verloren immer wieder die Verbindung zur LMC.
→ Wurde bei einem durch die LMC verwalteten Router über den WEBconfig-Tunnel in der LMC die Internet-Verbindung getrennt, führte dies zu einem unvermittelten Neustart des Routers.
→ Die Verwendung von mehr als einem gesteckten SFP-Modul des Typs ‚SFP-CO10MG' konnte zu einem unvermittelten Neustart des LANCOM Routers führen.
→ Einige Syslog-Zuordnungen zwischen Log-Level und Quelle waren falsch. So wurde z.B. dem Log-Level ‚Info' die Quelle ‚Notfall' zugeordnet.
→ Bei Verwendung von Mesh-VPN konnte es in Einzelfällen vorkommen, dass mehrere Prozesse gleichzeitig dieselben Variablen bearbeiteten. Dies führte zu einem unvermittelten Neustart des Routers.
→ Ein für Public Spot hochgelades Hintergrundbild wurde bei einer Größe von 1500 × 999 Pixel auf dem anzeigenden Gerät abgeschnitten, da die zugehörige Variable nur eine Länge von 16 Bit hatte.
→ Bei einem per LMC verwalteten LANCOM ISG-5000 konnten maximal 128 Public Spot-Benutzer angelegt werden.

VPN

→ Bei den Geräten LANCOM ISG-5000 und ISG-8000 wurde der VPN-Datendurchsatz falsch berechnet. In der Folge wurde ein von der Realität abweichender Wert auf der Konsole, im LANmonitor und der LMC ausgegeben.
→ Wenn über 1000 VPN-Verbindungen gleichzeitig aufgebaut wurden, belegte der ‚VPN-IKE'-Prozess alle freien CPU-Ressourcen und die CPU-Last des Routers stieg auf 100 % an. Dies führte dazu, dass der Aufbau der VPN-Verbindungen stoppte und Verbindungen teils aufgrund eines DPD-Timeouts auch wieder abgebaut wurden. In der Folge konnte ein großer Teil der VPN-Verbindungen nicht aufgebaut werden.

WLAN

→ Bei den Geräten LANCOM 1800EF und 1800VA wurde im Pfad ‚Status / WLAN-Management' ein hoher Wert für die Anzahl verbundener 6 GHz-WLAN-Clients angezeigt, obwohl auf diesen Geräte keine WLC Basic Option für Router aktiviert war.

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 10.80.0450 SU4

Korrekturen / Anpassungen

Allgemein

→ Es wurde eine Sicherheitslücke behoben, durch die nach Schreiben einer vollständigen Konfiguration (z. B. eine *.lcf Datei) mit einem weiteren Administrator mit Supervisor-Berechtigung das Passwort des Administrators ‚root' zurückgesetzt – und damit gelöscht - wurde.

LCOS-Änderungen 10.80.0448 RU3

Neue Features

→ Neue Konfigurationsmöglichkeit für Datenroaming in Fremdnetzen für Mobilfunkrouter auf der CLI. Datenroaming ist per Default aktiviert.

→ Neue Konfigurationsmöglichkeit für den PDP-Kontext (IPv4/IPv6) im Falle von Datenroaming in Fremdnetzen bei Mobilfunkroutern auf der CLI. IPv4 wird per Default beim Roaming in Fremdnetzen verwendet.

→ Der ICMP-SLA-Monitor generiert jetzt automatisch eine Syslog-Nachricht für Messungen bzw. Schwellwerte in der Ergebnisbewertung im Fall von ‚Kritisch' und ‚Warnung'.

→ Verbraucht ein laufender Trace zu viel freien Speicher, so wird dieser automatisch vom System beendet, sodass das Gerät davor geschützt wird, aufgrund von zu wenig freiem Speicher neu zu starten.

→ IPsec-Performanceverbesserung für den Fall, dass das Gerät die VPN-Verbindung aufgebaut hat (Initiator)

→ IPsec-Performanceverbesserungen für Geräte der 1800- / 1900-Serien

→ Der Syslog-Filter wird nun auch für Nachrichten des internen Syslog-Servers unterstützt.

Korrekturen / Anpassungen

Allgemein

→ Nach einem Konfigurations-Rollout über die LMC konnte es in speziellen Situationen vorkommen, dass die Änderungen wieder von der LMC übermittelt wurden. Dies führte dazu, dass die durch die LMC generierte Konfiguration fehlerhaft war und es beim erneuten Ausrollen zu einer inkonsistenten Konfiguration kam.

→ 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.

→ Wenn ein Dienst im LANCOM Router (z.B. DynDNS) noch TLS 1.0 oder 1.1 verwendete, führte dies zu einem unvermittelten Neustart.

→ Aufgrund eines zu großen DMA-Buffers konnte das Image eines LANCOM vRouters unter Microsoft Azure nicht installiert werden.

→ LANCOM Router der 1700-Serie mit fest konfigurierten Internet-Zugangsdaten, welche nachträglich an den ACS-Server der Deutschen Telekom angebunden wurden, sendeten einen falschen Provisionierungs-Code.

→ Weil der geforderte Wert im Übertragungsmodus für SFP-Verbindungen nicht hinterlegt war, wurde automatisch der Wert ‚Auto' hinterlegt. In der Folge wurde ein Konfigurations-Rollout über die LMC durch das Fehlen des Parameters verhindert.

→ Wenn der SMTP-Server eines E-Mail-Providers bei der TLS-Aushandlung nur den Verschlüsselungs-Algorithmus ‚secp384r1' zuließ, konnte der TLS-Handshake nicht abgeschlossen werden. Dies führte dazu, dass der E-Mail-Versand fehlschlug.

→ Wurde per LMC ein Addin-Skript ausgerollt, welches den Zeilen-Index fälschlicherweise auf 0 setzte (als Index dürfen nur Zahlen ab 1 verwendet werden), führte dies zu einem unvermittelten Neustart des Gerätes.

→ Bei Verwendung von Dynamic Path Selection in Verbindung mit einem Loadbalancer in der Zentrale wurde bei Ausfall einer VPN-Verbindung von der Zentral-Seite initiierter Datenverkehr einer bestehenden Session weiterhin über die abgebaute Verbindung geleitet. Dies führte dazu, dass die Pakete nicht durch die Filiale beantwortet werden konnten und somit kein Wechsel auf die andere VPN-Verbindung möglich war (passives Switchover).
In einem solchen Szenario leitet die Zentrale jetzt alle bestehenden Sessions über die andere VPN-Verbindung (aktives Switchover).

→ Der Load Score für Dynamic Path Selection wurde bei noch nicht aufgebauten Verbindungen auf den maximalen Wert von 250 statt auf 0 gesetzt.

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

→ Aufgrund der Einführung der ‚Japanese Unicode Conversion' in LCOS 10.80 mussten mehr Sonderzeichen berücksichtigt werden, was den DNS-Dienst deutlich stärker auslastete. In großen Szenarien konnte dies dazu führen, dass der DNS-Dienst die CPU dauerhaft zu 100 % auslastete und es dadurch zu Einschränkungen im laufenden Betrieb kam.

VPN

→ Es konnte vorkommen, dass VPN-Verbindungen nicht automatisch durch den Keepalive-Mechanismus aufgebaut wurden. Stattdessen wurde der Aufbau erst durch eine Datenübertragung ausgelöst.

→ Es konnte bei der Verwendung von Tunnel-Gruppen im VPN vorkommen, dass bei Abbau einer VPN-Verbindung auch die restlichen Verbindungen der Gruppe getrennt wurden.

→ Nach der Trennung mehrerer VPN-Verbindungen innerhalb einer Tunnel-Gruppe konnte es vorkommen, dass die neu aufgebauten Verbindungen nicht zu demselben Gateway aufgebaut wurden wie die restlichen Verbindungen. Dies führte dazu, dass die Kommunikation über den Loadbalancer nicht möglich war.

WLAN

→ In einem Public Spot-Szenario konnte es bei der Nutzung von selbst erstellen Willkommens-Seiten und Verwendung der Authentifizierungsmethode „Login nach Einverständniserklärung“ bei der ersten Anmeldung am System zu einer Fehlermeldung kommen, welche eine fehlende E-Mail-Adresse reklamierte.

VoIP

→ Im WEBconfig-Konfigurationsdialog zum Hinzufügen eines neuen DECT-Handsets fehlte das Feld zur Vergabe der Handset-ID.

LCOS-Änderungen 10.80.0345 RU2

Neue Features

→ Das Ping-Kommando kann über WEBconfig ausgeführt werden unter ‚Extras / Ping ausführen'.

→ Der Internet-Setup-Wizard für Mobilfunk wurde um Provider aus Frankreich, USA und den Niederlanden erweitert.

→ Das Broadcast-Bit für den DHCP-Client ist nun schaltbar. Dazu gibt es in der WAN-Layer-Tabelle auf der Konsole bzw. im LCOS-Menübaum den Parameter ‚B-DHCP' in der Auswahl für Layer 3.

→ Anpassungen beim QinQ VLAN auf dem WAN: Es wird nun das Szenario unterstützt, dass beide Ethertypes (z.B. 0×8100) identisch sind, aber nur ein Tag enthalten ist, bzw. ‚0' ist.

→ Es werden weitere Statusparameter für Mobilfunk im TR-069-Datenmodell TR-181 unterstützt.

→ Unterstützung für die Anzeige der WWAN-Firmwareversion in der LMC.

→ Beim LANCOM ISG-8000 können auf der Konsole Parameter wie Hintergrundbeleuchtung für das Geräte-Display konfiguriert werden.

→ In der VCM-Status-Tabelle ‚Line' wird nun auch das verwendete Interface bzw. die WAN-Verbindung für die SIP-Registrierung angezeigt.

Korrekturen / Anpassungen

Allgemein

→ Bei hohem IPSec-Datenaufkommen konnte es vorkommen, dass Enqueue-Fehler auftraten, wenn Pakete einer Queue hinzugefügt werden sollten, die bereits freigegeben wurden. In Einzelfällen konnte dies in Verbindung mit weiterem verschlüsseltem Datenverkehr (z.B. HTTPS) zu einem unvermittelten Neustart des Routers führen.

→ Der vRouter unterstützt nur einen CPU-Kern. Es konnte allerdings vorkommen, dass der vRouter mehreren virtuellen CPU-Kernen Jobs zuwies, was dann zu einem unvermittelten Neustart führte.

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

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

→ Bei einer TACACS+-Anmeldung war es nicht möglich, Benutzernamen mit mehr als 16 Zeichen zu verwenden. Benutzernamen können jetzt bis zu 32 Zeichen enthalten.
→ 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.
→ 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.
→ 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.
→ Bei Verwendung des Testmodus (flash no) konnte es in Einzelfällen vorkommen, dass nach dem Schreiben einer Konfiguration die vollständige Geräte-Konfiguration gelöscht wurde.

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.

WLAN

→ Nach einem Update auf LCOS 10.80 funktionierte die PoE-Aushandlung per LLDP nicht mehr. Dies führte dazu, dass Access Points, welche für die volle Funktionalität PoE nach 802.3at benötigen, lediglich mit PoE nach 802.3af versorgt wurden. Dadurch wurde die Funktionalität der Access Points eingeschränkt.
→ Bei Verwendung des Public Spot-Modus ‚Anmeldedaten werden über SMS versendet' konnte auf der Landing-Page keine Ländervorwahl ausgewählt werden.

VoIP

→ 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 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.

→ Empfing der Voice Call Manager im INVITE vom SIP-Provider zwei alternative Media-Streams (m=audio) mit unterschiedlichen Ports, antwortete der Router im „200 OK" an den Provider nur mit einem Media-Stream. Dies führte dazu, dass das Telefonat vom SIP-Provider abgebaut wurde.

→ In einem Szenario mit angebundener SIP-TK-Anlage sendete der Voice Call Manager nach Weiterleitung eines eingehenden Telefonates an einen externen Teilnehmer per SIP302 fälschlicherweise ein CANCEL an die SIP-TK-Anlage.

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

LCOS-Änderungen 10.80.0233 RU1

Neue Features

→ Unterstützung der Zero Touch-Inbetriebnahme für die LANCOM 1800 Blackline-Serie und LANCOM 1900-Serie am WAN-Ethernet-Port. Hierzu muss das Gerät mit LCOS 10.80 RU1 oder höher ausgeliefert werden oder es muss nach dem Update auf LCOS 10.80 RU1 ein Reset durchgeführt werden.

→ Die Betriebsart für den Rollout-Agent ist im Default nun ‚Aus'.

→ Im Syslog werden nun für WWAN erweiterte Informationen bei einer Verbindungstrennung angezeigt.

→ Bei der Anzeige von Tabellen mit vielen Einträgen in der WEBconfig werden die Einträge nun auf mehreren Seiten durch Paginierung angezeigt.

Korrekturen / Anpassungen

Allgemein

→ 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.

→ 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.

→ 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.

→ Die 4G-LED des LANCOM 1800VA-4G leuchtete dauerhaft blau, auch wenn das Mobilfunk-Modul nicht aktiv war.

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

→ 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 nicht gelöscht wurden, wenn die Verbindung abgebaut war. Dadurch konnten die L2TP-Verbindungen nicht erneut aufgebaut werden.
→ OpenSSL wurde auf die Version 3.0.12 aktualisiert.

WLAN

→ Bei Access Points mit festem Frequenzband auf einem WiFi6-WLAN-Modul konnten per WEBconfig verschiedene Frequenzbänder ausgewählt werden.
→ In LCOS 10.80 Rel funktionierten aufgrund von Änderungen an den Pfaden für die jquery-Bibliotheken die Public Spot Templates nicht mehr.
Es gibt jetzt neue Variablen für die jquery-Bibliotheken und neue Public Spot Templates. Sofern mit LCOS ab Version 10.80 RU1 eigene Templates verwendet werden sollen, müssen zwingend die neuen Versionen eingesetzt werden.

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.
→ Die 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.
→ Per WEBconfig konnten keine Zertifikats-Container (PKCS12) in einen der VPN-Zertifikats-Slots hochgeladen werden. Der Vorgang wurde immer mit den Meldungen „Upload fehlgeschlagen" und „Falsches Passwort oder ungültiger Dateityp" quittiert.

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.

LCOS-Änderungen 10.80.0155 Rel

Neue Features

→ Unterstützung der Re-Init-Funktion für 5G-Module

→ Unterstützung für N:N NAT bei Multicast-Datenpaketen (nicht für SSM)

→ Unterstützung für WWAN-Status Werte RSRP, RSRQ und SINR und Darstellung im WEBconfig-Dashboard

→ Verbesserung der Festplattenperformance des LANCOM vRouters

Korrekturen / Anpassungen

Allgemein

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

→ 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'.

→ Nach einer undefinierten Zeit (es konnten mehrere Wochen sein), schaltete sich das WWAN-Modul selbständig ab und war dann im Status ‚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.

→ 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.

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

→ 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.

→ Bei einigen LANCOM Mobilfunk-Routern lieferte das verbaute WWAN-Modul keine Netzwerkkennung in Textform. In der Folge blieb das ‚Network'-Feld nach einer Abfrage (z.B. per CLI mit ‚ls /Status/Modem-Mobile') leer.

IKEv2-Verbindung. Dabei konnte es vorkommen, dass der Speicher der gelöschten Child SA doppelt belegt wurde. Dies führte zu einem unvermittelten Neustart des Routers.

→ 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

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

→ 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.

→ 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.

→ Trat ein ‚Framing Error' auf dem seriellen Bus zum ePaper-Funkmodul auf, führte dies dazu, dass die Verbindung zu den ePaper-Displays abbrach und die Displays nicht mehr aktualisiert werden konnten. Im Syslog der Access Points wurden in einem solchen Fall die Fehlermeldungen „AccessPoint - An error occurred, need to restart WePaper Access-Point" und „SerialInterface - Error in communication with RF-Module!" ausgegeben.
Die Verbindung zwischen dem ePaper-Funkmodul und den ePaper-Displays wird jetzt auch ohne einen Neustart des Access Points wieder hergestellt.

VoIP

→ 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.

→ 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 der 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.

LCOS-Änderungen 10.80.0124 RC2

Neue Features

→ Der DHCPv4-Client untestützt die Option MTU.

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.

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

→ Die IPv6-Firewall verwendete ein nicht vorhandenes Content-Filter-Profil ‚CF-PARENTIAL-CONTROL-PROFILE' statt ‚CF-PARENTAL-CONTROL-PROFILE'.

→ Im Pfad ‚Setup/Mail' wurden veraltete SSL/TLS Standard-Einstellungen verwendet. Es werden jetzt folgende Standard-Werte genutzt:

- mindestens TLS 1.2
- kein MD5/SHA1
- kein 3DES
- ausschließlich Key Agreement mit PFS

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

→ Der TR-069-Dienst sendete seine Anfragen mit der IP-Adresse statt des DNS-Namens 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.

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.

LCOS-Änderungen 10.80.0075 RC1

Neue Features

→ Unterstützung von Let‘s Encrypt-Zertifikaten (ACME-Client) für WEBconfig und den LANCOM Public Spot

→ Zero-touch-Rollout für Mobilfunk-Router zusammen mit der LMC

→ WEBconfig im neuen Corporate Design

→ Unterstützung von Google Cloud (GCP) für den LANCOM vRouter

→ Unterstützung der High Availability Clustering Option L für die LANCOM 1900-Serie

→ Router können Traces und Wireshark-Captures direkt auf einem USB-Stick aufzeichnen und speichern.

→ Einträge in der Aktionstabelle können durch ein CLI-Kommando getestet bzw. ausgeführt werden.

→ Unterstützung der Funktion ‚Automatischer APN‘ bei Mobilfunk-Routern

→ Der Zugriff auf RPCap und LCOScap über WAN kann konfiguriert werden.

→ Der GPON-Status kann im WEBconfig-Dashboard angezeigt werden.

→ Das GPON-Passwort kann nun auch im HEX-Format (20 Zeichen) eingegeben werden.

→ Das Accounting im Router wurde überabeitet und kann jetzt auch zur Anzeige des Durchsatzes aktueller Sessions von Stationen im Analyse-Fall verwendet werden.

→ Unterstützung von konfigurierbaren Reaktionen auf eingehende SMS bei Mobilfunk-Routern, z. B. Versenden von Antwort-SMS für das Nachbuchen bei verbrauchtem Datenvolumen

→ Unterstützung von Cold-Standby bei Mobilfunk-Routern

→ Die Eingabemöglichkeit für das Hauptgerätepasswort und weitere Administratoren wurde auf maximal 128 Zeichen erweitert. Bei Nutzung der neuen Passwortlänge ist ein Downgrade auf ältere LCOS-Versionen nicht mehr möglich.

→ Die Status-Tabelle ‚Protocol-Table‘ unter ‚/ Status / IP-Router‘ entfällt.

→ Der Schalter ‚LTE-Delayed-Attach‘ bei Mobilfunk-Routern entfällt.

→ Der Status-Zähler ‚Stack-Errors‘ des IP-Routers entfällt.

→ Die Status-Tabelle ‚Establish-Table‘ entfällt.

→ Die Spalten ‚Tx-normal‘, ‚Tx-urgent‘ und ‚Tx-reliable‘ in der Tabelle ‚/ Status / WAN / Packet-Transport‘ entfallen.

→ Die Unterstützung für SSL 3.0 sowie Cipher mit 56 Bit oder weniger wurde entfernt.

→ Die Unterstützung für 3G (USB-)WWAN-Modems wurde vollständig entfernt.

→ Von LCOS erzeugte WEBconfig-Zertifikate haben nur noch eine maximale Gültigkeit von 365 Tagen.

→ Das Deaktivieren von Syslog deaktiviert nun auch das regelmäßige Schreiben des Syslog-Backups in den internen Flash-Speicher.
→ DHCP- und DHCPv6-Server werden in WEBconfig unter ‚Dienste' angezeigt.
→ Das ‚(VLAN-)Priority Bit' kann bei WAN-Verbindungen gesetzt werden.
→ Beim DHCP-Client können zusätzliche DHCP-Optionen konfiguriert werden.
→ Beim DHCPv6-Client können zusätzliche DHCPv6-Optionen konfiguriert werden.
→ Unterstützung für Interim-Accounting im Netflow
→ Netflow verwendet nun intern 64 Bit-Zähler.
→ Unterstützung von Dual Stack (IPv4 / IPv6) im Config Mode bei IKEv2 gegen den LANCOM Advanced VPN Client

Korrekturen / Anpassungen

Allgemein

→ Bei Routern mit Multicore-CPU (z. B. LANCOM 1800er-Serie) wurde im Konsolen-Pfad ‚Status / Hardware-Info' lediglich die Auslastung für den CPU-Core 0 angezeigt. Es wird jetzt der Mittelwert aller CPU-Cores angegeben.
→ Nach Aktivierung einer VPN-25-Option auf einem Router (kein Neustart erforderlich) konnte bei aktivierter CA das Geräte-Zertifikat über die Option ‚Aktuelles CA Zertifikat herunterladen' nicht in WEBconfig heruntergeladen werden. Der Vorgang wurde mit der Fehlermeldung „Not found" quittiert. Der Download des Zertifikats war erst nach einem Neustart möglich.

VoIP

→ Empfing der Voice Call Manager in einem INVITE von einer SIP-TK-Anlage sowohl die P-Asserted-Identity (PAI) als auch die P-Prefered-Identity (PPI), verwendete der Voice Call Manager anschließend die Rufnummer in der PAI. Wenn diese Rufnummer in einem Szenario mit CompanyFlex-Anschluss dem SIP-Provider nicht bekannt war (etwa wegen einer fehlenden Ziffer), wurde das Telefonat abgebaut und mit der Fehlermeldung „403 Forbidden“ quittiert. Es gibt jetzt im Pfad ‚Setup / Voice-Call-Manager / Users / SIP-Users / Users‘ den zusätzlichen Parameter ‚Prefer-Identity-Field‘. Mit diesem kann ausgewählt werden, ob die PAI (Prefer-PAI) oder die PPI (Prefer-PPI) präferiert werden soll (Standardeinstellung ist wie bisher PAI).

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.