LANCOM Release Notes

LCOS

10.40 RU1

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

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

27.08.2020, CBuersch

Inhaltsübersicht

LANCOM Systems

1. Einleitung

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

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.40 RU1 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 6 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite
https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/

2. Gerätespezifische Kompatibilität zu LCOS 10.40

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten.
Auch für Geräte, die keine aktuelle LCOS-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstütze LCOS-Version für Ihr Gerät finden Sie unter
https://www.lancom-systems.de/produkte/firmware/lifecycle-management/produkttabellen/

Mit LCOS 10.40 entfällt die Unterstützung für folgende Geräte

- LANCOM 1780EW-4G
- LANCOM 1781A-4G
- LANCOM L-322E
- LANCOM L-1302acn
- LANCOM L-1310acn

3. Hinweise zu LCOS 10.40

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.

4. Feature-Übersicht LCOS 10.40

4.1 Feature-Highlights

Next-Generation SD-WAN: LANCOM High Scalability VPN (HSVPN)

High Scalability VPN verbessert deutlich die Skalierbarkeit und Effizienz Ihrer SD-WAN-Architektur. Wo zuvor für jede Anwendung ein einzelner VPN-Tunnel benötigt wurde, transportiert HSVPN beliebig viele Netze in einem einzigen VPN-Tunnel gesammelt an die Gegenstelle – dabei bleibt jedes Netz sicher und strikt voneinander getrennt. Der Vorteil für Ihr Business: deutlich weniger benötigte VPN-Tunnel sowie schnellere Wiederherstellungszeiten bei Failover.

Modernes Look & Feel: Neue WEBconfig

Erfreuen Sie sich nun an einem ganz neuen Look & Feel in der LANCOM WEBconfig. Angelehnt an das moderne und helle Design der LANCOM Management Cloud wurde die WEBconfig komplett neu überarbeitet und bietet Ihnen eine attraktive und frische Optik..

Multicast Routing

Ab sofort werden Multicast-Daten, wie z. B. IPTV, effizient an verschiedenen Endgeräte übertragen. Während bislang an jeden Empfänger separate Datenpakete verschickt werden mussten, ermöglicht Multicast-Routing die parallele Übertragung eines IP-Stroms an mehrere Empfänger. Dadurch wird die Last für den Router verringert und die verfügbare Routing-Kapazität besser genutzt.

4.2 Weitere Features

SD-WAN Zero-touch Deployment für DSL-Router

Automatische Inbetriebnahme von DSL-Routern an BNG-Telekom-Anschlüssen mit der LANCOM Management Cloud – ohne die aufwändige Konfiguration von DSL-Zugangsdaten auf dem Router.

Netflow

Mit Netflow können Informationen zur Netzwerkanalyse über eingehenden bzw. ausgehenden IP-Datenverkehr (u.a. Quelle, Ziel, Ports) im Router an einen zentralen Server zur Auswertung gesendet werden.

IKEv2-VPN mit Windows-Login

Mobile VPN-Clients können jetzt mittels IKEv2 EAP gegen eine zentrale Datenbank wie Microsoft Active Directory oder RADIUS authentifiziert werden, ohne dass die VPN-Zugangsdaten auf dem LANCOM Router gespeichert werden müssen.

Mehr Flexibilität bei Backup-Szenarien

Die Priorisierung von Routen bietet neue Möglichkeiten für flexible Backup-Szenarien

Neue SD-WAN-Funktionen für den Loadbalancer

Auf zentralseitigen Gateways können VPN-Loadbalancer durch RADIUS automatisch erzeugt werden. Zudem werden mehrere VPN-Kanäle zu Tunnel-Gruppen zusammengefasst, sodass auch im Fall eines Failovers der VPN-Aufbau zu einem gemeinsamen Gateway erfolgt.

WLAN-Zeitsteuerung

Ermöglicht das zeitgesteuerte Aktivieren und Deaktivieren von SSIDs im WLAN. Ideal für WLAN-Netze, die nur zu bestimmten Zeiten zur Verfügung stehen sollen, wie beispielsweise Hotspots oder WLAN in Bildungseinrichtungen.

Mehr Sicherheit im VPN

Unterstützung von neuen und modernen Verschlüsselungs-Algorithmen wie Chacha20-Poly 1305, Digital Signature mit ECDSA sowie neue Diffie-Hellmann-Gruppen.

TLS 1.3 Client Mode

Die Unterstützung des neuen Protokolls TLS 1.3 erhöht die Sicherheit beim Zugriff des Routers auf Webdienste.

Neue Filter für individuelle Meldungen

Konfigurierbare Filterlisten für SNMP-Traps und SYSLOG ermöglichen den Erhalt individualisierter Monitoring-Meldungen.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 5 „Historie LCOS 10.40“.

5. Historie LCOS 10.40

LCOS-Änderungen 10.40.0291 RU1

Korrekturen / Anpassungen

Allgemein

- Ein im Konfigurations-Menü ‚Kommunikation / Protokolle / Polling-Tabelle' eingerichtetes ICMP-Polling funktionierte nicht, wenn das Ping-Intervall auf 0 gesetzt war (Standard-Wert).
  Das bisherige Verhalten wurde wieder hergestellt. Ist den Parametern ‚Ping-Intervall' und ‚Wiederholungen' der Wert 0 zugewiesen (Standard-Werte), wird ein Standard-Intervall von 20 Sekunden bei 5 Wiederholungen verwendet.
- Die Funktion Netflow ließ sich auf Access Points und WLAN-Controllern nicht aktivieren, obwohl das Menü in LANconfig zur Verfügung steht. Netflow konnte nur auf einem Router aktiviert und verwendet werden. Die Funktion ist jetzt auch auf Access Points und WLAN-Controllern implementiert.
- Die Layer-7-Anwendungserkennung funktionierte nicht, wenn diese über die zugehörige VLAN-Tabelle (Setup/Layer-7-App-Detection/VLAN/) auf ein bestimmtes VLAN eingeschränkt wurde.
- Die Konfiguration konnte auf einen durch die LMC verwalteten Router nicht ausgerollt werden, wenn gleichzeitig ein neues Objekt in der DNS-Ziel-Liste angelegt und dieses in einer neuen Firewall-Regel referenziert wurde.
- Statische Routen, deren Next-Hop auf ein LAN-Interface verwies, wurden nicht korrekt aktualisiert. Der Status verblieb auf ‚Static Down', wodurch die Default-Route anstelle der statischen Route verwendet wurde. Dies betraf sowohl IPv4 als auch IPv6.
  Dies konnte dazu führen, dass VPN-Verbindungen nicht aufgebaut werden konnten.
- N:N-NAT funktionierte nicht, da ein ARP-Request für die umgesetzte IP-Adresse vom Router nicht beantwortet wurde.
- Wenn für einen GRE-Tunnel ein Routing-Eintrag erstellt wurde, welcher auf eine IP-Adresse aus einem lokalen Netzwerk verwies, konnte der GRE-Tunnel nicht aufgebaut werden.
- Empfing der Router ein DNS-Paket mit einem SOA-Record ohne Inhalt (Datenlänge 0), wurde dieses Paket mit der Meldung „got malformed DNS packet" verworfen. DNS-Pakete mit einem SOA-Record ohne Inhalt werden jetzt vom DNS-Forwarder und vom DNS-Client angenommen.
- Ein DNS-Paket, in dem ein Pointer auf einen weiteren Pointer zeigte, wurde vom Router mit der Meldung „got malformed DNS packet" verworfen. Es werden jetzt DNS-Pakete mit maximal vier Pointer Hops pro Record angenommen.
- Die Kommunkation mit einem externen Syslog-Server über einen benutzerdefinierten Port (ungleich 514) war unabhängig vom genutzten Protokoll (TCP oder UDP) nicht möglich. Der Router ignorierte die Einstellung und nutzte weiterhin den Port 514.
- Bei Ausfall einer Internet-Verbindung wird versucht, diese wieder aufzubauen, wodurch sie in den Status ‚Protocol' wechselt. In einem Backup-Szenario mit der ‚Administrativen Distanz' wurde der konfigurierte Wert für diese beibehalten, da aufgrund der Protokollaushandlung die Verbindung als aufgebaut interpretiert wurde.
  Dies führte dazu, dass die zweite Route bei Ausfall der Haupt-Verbindung nicht aktiv geschaltet wurde.

VPN

- Wurde in WEBconfig ein neuer VPN-Einwahl-Zugang für den Advanced VPN Client mit dem Setup-Assistenten ‚Einwahl-Zugang bereitstellen (RAS, VPN)' angelegt, führte dies dazu, dass bereits vorhandene Einwahl-Zugänge von diesem gelöscht wurden.
- Ein Zugriff über eine VPN-Verbindung auf die WAN-IP-Adresse des Routers mit Portforwarding auf eine Ressource im lokalen Netzwerk (Hairpin-NAT) funktionierte nicht, da bei dem Portforwarding das Paket wieder in das WAN geleitet wurde.
- Eine IPv6 VPN-Verbindung mit UDP-Verschlüsselung war nicht funktionsfähig, da die Pakete an den IPv4 ESP-Dienst weitergeleitet wurden.

WLAN

- Bei Verwendung des Features ‚Fast Roaming' konnte es bei der Übertragung des PMK per IAPP vorkommen, dass der PMK bei Access Points mit zwei WLAN-Modulen und gleicher SSID auf beiden Modulen nur in den PMK-Cache einer BSSID übernommen wurde. Ein Roaming-Vorgang auf das WLAN-Modul eines solchen Access Points ohne PMK führte dazu, dass die Fast Transition mit der Fehlermeldung „R0KH unreachable" abgelehnt wurde.
- Es konnte in Einzelfällen vorkommen, dass auf einem WLAN-Controller Prozesse zur Verwaltung von Access Points (CAPWAP-Worker) nicht korrekt beendet und daher System-Ressourcen nicht wieder freigegeben wurden. Dies konnte zu einem unvermittelten Neustart des Gerätes führen.
- Baute ein Access Point im Client-Betrieb eine WLAN-Verbindung zu einem weiteren Access Point im Modus ‚Basisstation' auf, konnten Netzwerk-Teilnehmer, die mit jeweils einem der Access Points verbunden waren, nicht untereinander kommunizieren, wenn auf der Basisstation VLAN aktiv war und auf dem Client nicht.
- Wenn mehrere Access Points gleichzeitig in Betrieb genommen wurden und eine automatische Kanalwahl konfiguriert war, wurde für alle Access Points der gleiche Kanal gewählt. Die automatische Kanalwahl wurde nun so optimiert, dass unterschiedliche Kanäle verwendet werden.

VoIP

- Ein von einem SIP-Benutzer initiiertes ausgehendes Telefonat mit unterdrückter Rufnummer konnte nicht aufgebaut werden, da das Telefonat keinem Benutzer zugeordnet werden konnte.
- Es konnte vorkommen, dass der LANCOM Router im ‚183 Session Progress' an den Provider das Flag ‚Require: 100rel' verschickte, obwohl der verbundene SIP-Teilnehmer dies nicht unterstützte und auch nicht im RINGING bekanntgegeben hatte. Der SIP-Teilnehmer quittierte dies mit der Fehlermeldung ‚500 Server Internal Error', womit es zu einem Abbruch des Telefonates kam.
- Der Voice Call Manager startet das RTP-Monitoring in der ‚Early Media Phase'. Nach Ablauf des Timers wird das RTP-Monitoring deaktiviert, wenn RTP-Pakete erkannt wurden. Der Voice Call Manager erwartet in diesem Fall einen externen Freiton.

  Brach der RTP-Datenstrom ab, erkannte der Voice Call Manager dies nicht und konnte dadurch auch keinen lokalen Freiton generieren.

- Wurde einem ISDN-Benutzer als interne Rufnummer die Anschluss-Rufnummer + # zugewiesen (z.B. 12345#) und als MSN die # (z.B. die 33), konnte von diesem ISDN-Benutzer kein ausgehendes Telefonat aufgebaut werden, da für den Rufaufbau die MSN verwendet wurde anstatt die MSN an die interne Rufnummer anzuhängen (z.B. 1234533).
- In einem Szenario mit einer Netphone TK-Anlage im Bridge Mode kam ein Telefonat nur mit dem Codec G.711 zustande, obwohl im ersten Invite G.722 verwendet wurde.

LCOS-Änderungen 10.40.0210 Rel

Korrekturen / Anpassungen

Allgemein

- Die Routing-Option ‚ICMP-Redirect senden' war ohne Funktion.
- SNMPv3-Traps wurden in einem nicht konformen Format gesendet, was dazu führte, dass Statusanzeigen und Werteänderungen z.B. im LANmonitor nicht angezeigt wurden.
- Es wurden mehrere Fehlverhalten im Zusammenhang mit SNMP-Zugriffen auf ein LANCOM Gerät (z.B. Öffnen im LANmonitor) behoben, da das SNMP mit der neuen Passwort-Hash-Funktion nicht fehlerfrei zusammenarbeitete.
- In der Whitelist des LANCOM Content-Filter (Menü ‚Content-Filter / Profile / Whitelist-Adressen') konnten mit LANconfig zwar neue Einträge hinzugefügt werden, diese wurden jedoch beim Zurückschreiben nicht in die Konfiguration übernommen.
- Es konnte bei Verwendung von GRE-Tunneln vereinzelt zu einem unvermittelten Neustart kommen, wenn ein aufgebauter GRE-Tunnel einen ungültigen Verbindungs-Kanal an das LCOS meldete.
- Wenn im WEBconfig ein Zertifikat erstellt wurde, welches als Information eine E-Mail-Adresse (E) enthielt, wurde das Zertifikat nicht erzeugt.
- Nach der Deaktivierung der Funktion ‚Klartext-Passwort erhalten' musste bei einer Anpassung der ‚Weiteren Administratoren' (etwa die Funktions-Rechte) immer auch das jeweilige Passwort mit eingegeben werden. Ansonsten wurde die Fehlermeldung „Ihre Eingabe für ‚Passwort' ist fehlerhaft" ausgegeben.
  Weiterhin konnte es dazu kommen, dass ein leeres Passwort gesetzt wurde, wenn die Funktion ‚Geräte-Passwort-Richtlinie erzwingen' deaktiviert war.
- Auf einem durch die LMC verwalteten Gerät konnte es nach der Zertifikats-Erneuerung durch den LMC-Client sporadisch zu einem unvermittelten Neustart kommen.
- VLAN-IDs wurden bei Verwendung von IPv6 nicht übertragen, wenn die VLAN-ID in den IPv6-Netzwerken hinterlegt wurde, aber das VLAN-Modul nicht aktiv war. Dies führte zu Problemen bei der Kommunikation.
- Eingehende Pakete von einer Internet-Verbindung mit Routing-Tag ‚0' wurden nicht an eine DMZ mit einem von ‚0' abweichenden Tag weitergeleitet.
  Die Behandlung wurde jetzt so abgeändert, dass eine DMZ aus allen Netzwerken erreichbar ist, also auch aus dem Internet. Dies entspricht dem Verhalten in bisherigen LCOS-Versionen.
- Die Kommunikation zwischen zwei Netzwerken war bei Verwendung mehrerer potentiell passender Firewall-Regeln nicht möglich, wenn beim Aufbau der Session nicht die erste dieser Firewall-Regeln zutraf, sondern erst eine nachfolgende Regel. Dadurch wurde als Ziel für das Paket das Gateway der Internet-Verbindung verwendet.
- Bei gleichzeitiger Verwendung von BGP und OSPF wurden per BGP gelernte Routen nicht an den OSPF-Nachbarn weitergeleitet, wenn die Weiterleitungs-Adresse nicht über einen Intra- oder Inter-Area-Pfad erreichbar war. Die Weiterleitungs-Adresse wird jetzt per Default auf 0.0.0.0 gesetzt.
- Wurde ein Paket aus einem lokalen Netzwerk an die IP-Adresse des Routers in einer DMZ gesendet, wurde dieses von der Firewall des Routers abgelehnt, wenn als Verbindungsziel die Internet-Gegenstelle der DMZ in der Firewall-Regel hinterlegt war.
  Wird eine IP-Adresse des Routers angesprochen (Loopback), wird das Ziel-Interface jetzt nicht mehr in der Firewall überprüft.

- Bei den Geräten der LANCOM OAP-170xB-Serie wurden negative Temperaturmesswerte vom Temperatursensor falsch behandelt, was dazu führen konnte, dass ein WLAN-Modul aufgrund eines falsch ermittelten Temperaturwertes abgeschaltet wurde.
- Die LL2M-Funktion konnte nicht genutzt werden, wenn für das angesprochene Gerät kein Passwort in der Konfiguration gesetzt war.

VPN

- Eine IKEv2-Verbindung konnte über eine PPPoE- und PPTP-Internet-Verbindung nicht aufgebaut werden, da die ausgehandelte MTU nicht an die Kontroll-Ebene des Routers weitergeleitet wurde und die MTU im VPN daher zu groß gewählt wurde.
- Gab es mehrere nicht komplett ausgehandelte VPN-Regeln (IKE_SA) für eine RAS-VPN-Einwahl, wurde die übergeordnete Regel-Liste für diese VPN-Verbindung nach Ablauf der ersten dieser Regeln gelöscht. Versuchte der Router anschließend trotz fehlender Regel-Liste ein DPD-Paket an den RAS-VPN-Client zu senden, führte dies zu einem unvermittelten Neustart des Routers.
  Dies konnte auftreten, wenn der RAS-VPN-Client fehlerhaft konfiguriert war und auf IKE_AUTH-Response Pakete des Routers nicht antwortete und stattdessen einen erneuten Verbindungsaufbau startete.
- In einem Szenario mit aktivem VPN-Loadbalancer konnte es bei gleichzeitigem Aufbau mehrerer VPN-Verbindungen vom gleichen Einwahl-Router (wird durch die LMC so konfiguriert) vorkommen, dass bei Neuaushandlung der DH-Gruppe nach 30 Sekunden ein Timeout einer noch nicht aufgebauten VPN-Verbindung auftrat. Dies führte dazu, dass auch alle bisher aufgebauten VPN-Verbindungen auf dem Einwahl-Router abgebaut wurden.
- Wenn sich die Authentifizierungsmethoden zwischen einer Haupt-VPN-Verbindung und einer weiteren VPN-Verbindung, welche als Backup-VPN-Verbindung konfiguriert ist, unterschieden (z.B. zertifikatsbasiert bei Hauptverbindung und PSK bei Backup-Verbindung) wurde im Backup-Fall die Backup-VPN-Verbindung nicht aufgebaut.
- Wurde bei einem Cron-Job eine VPN-Site-to-Site-Verbindung von der Gegenseite getrennt, hatte dies zur Folge, dass auch einige bestehende Client-to-Site-VPN-Verbindungen getrennt wurden.
- Bei VPN-Verbindungen war der Zähler für empfangene IP-Pakete (Rx-Packets Counter im Pfad ‚Status / VPN') ohne Funktion.

WLAN

- Wenn bei einem LANCOM WLAN-Controller in einem Access Point-Profil für ein Gerät der LN-17xx-Serie 2,4 GHz-Kanäle auf dem Funkmodul 1 explizit ausgewählt wurden, setze der Access Point die Kanal-Liste so um, dass auf dem zweiten Funkmodul ein nicht existierender 5 GHz-Kanal verwendet wurde.
- Access Points konnten aufgrund eines Fehlers bei der DTLS-Aushandlung nicht durch einen WLAN-Controller im vRouter (vWLC) verwaltet werden.
- Wurde auf einem LANCOM IAP-821 der Setup-Assistent ‚WLAN konfigurieren' ausgeführt, die WLAN-Betriebsart auf ‚Client' gesetzt und das Feature ‚Soft-Roaming' deaktiviert, kam es nach Fertigstellen des Setup-Assistenten zu einem unvermittelten Neustart. Wenn eine Konfigurationsdatei mit deaktiviertem Soft-Roaming in einen LANCOM IAP-821 hochgeladen wurde, kam es ebenfalls zu einem unvermittelten Neustart.

VoIP

- Wenn sich ein SIP-Client über eine VPN-Verbindung per SIP-ALG registrieren sollte, so schlug der Registrierungsvorgang fehl.
- Es konnte sporadisch vorkommen, dass ein beendeter analoger Anruf im LANCOM Router weiterhin als aktiv geführt wurde. Wenn die ‚Busy on Busy'-Funktion (Ruf abweisen bei besetzt) verwendet wurde, führte dies dazu, dass eingehende analoge Anrufe abgewiesen wurden.
- Wenn bei konfigurierter E-Mail-Benachrichtigung ein per ISDN eingehender Anruf nicht angenommen wurde, schlug die E-Mail-Benachrichtigung fehl.

LCOS-Änderungen 10.40.0166 RC3

Korrekturen / Anpassungen

Allgemein

- Die Konfiguration des Gerätes konnte in LANconfig nicht zurückgeschrieben werden, wenn die Option ‚Erzwinge Passwort Regeln' unter ‚Meldungen/Monitoring / Protokolle / SNMP-Einstellungen' initial aktiviert war und diese anschließend deaktiviert sowie im gleichen Schritt ein SNMP-Benutzer angelegt wurde.
- Wurde auf einem vRouter ein Port-Forwarding für den UDP-Port 500 (IKE) eingerichtet und aktiviert, konnte dieser selbst keine VPN-Verbindung mehr aufbauen.
- In Einzelfällen konnte es bei einem Zugriff auf einen LANCOM Router per WEBconfig über das Protokoll TLS 1.3 zu einem unvermittelten Neustart kommen.
- Wenn eine LAN-Verbindung zu einem Switch physikalisch entfernt wurde (durch Ziehen des Ethernet-Steckers am Router oder Switch), rief der LANCOM Router das zugehörige LAN-Netzwerk über RIP korrekterweise zurück, es wurde jedoch nach wiederhergestellter LAN-Verbindung nicht erneut publiziert.
- Bei einem UDP-Scan im Internet werden innerhalb einiger Sekunden mehrere Tausend Pakete von einer festen Quell-IP-Adresse mit einem festen UDP-Quell-Port an eine beliebige Ziel-IP-Adresse an einen größeren UDP-Ziel-Port-Bereich geschickt.
  Wenn die Ziel-IP-Adresse Bestandteil der DMZ eines LANCOM Routers war, d. h. die Pakete wurden geroutet, war der Router anschließend sehr stark ausgelastet und gegebenenfalls mehrere Minuten mit der Verarbeitung der Pakete beschäftigt.

VPN

- In großen Szenarien mit mehreren VPN-Konzentratoren konnte es bei Verwendung von IKEv2-Einwahl-Verbindungen vereinzelt vorkommen, dass die VPN-Verbindung in der Zentrale nicht korrekt terminiert wurde, wenn der einwählende Router (Initiator) seine VPN-Verbindung verlor (z.B. nach einem DPD-Timeout oder einer Zwangstrennung der Internet-Verbindung).
  Wenn der erneute Verbindungsversuch mit einem anderen VPN-Konzentrator in der Zentrale erfolgte, verblieb die Verbindungs auf dem ersten Konzentrator im Status ‚Connect', was dazu führte, dass bei Verwendung eines Routing-Protokolls (z.B. BGP) eine Route propagiert wurde, welche auf eine nicht mehr existierende VPN-Verbindung verwies.

WLAN

- Bei der Verwendung von WLC-Tunneln wurden bei der Kommunikation von WLAN-Geräten innerhalb derselben SSID, welche auf unterschiedlichen Access Points eingebucht waren, die Pakete in der LAN-Bridge mit der Meldung ‚no forward to interface itself' abgelehnt.
- Im 2,4 Ghz-Betrieb (802.11g/n gemischt) wurden WLAN-Management-Pakete zur Bekanntgabe der SSID und Annahme von WLAN-Geräten (sogenannte ‚Beacons') mit einer Datenrate von 1 MBit/s anstatt 6 MBit/s versendet. Aufgrund der deutlich höheren Paketanzahl stieg die Kanallast stark an und konnte somit zu geringeren erzielbaren Datenraten im WLAN führen.

VoIP

- Bei einem eingehenden Anruf wurde der Contact Header nicht in das ‚180 Ringing' an den Provider eingepflegt. Dies führte bei MagentaZuhause Regio-Anschlüssen dazu, dass ein externer Anrufer kein Klingeln hörte.
- Ein durch den Provider generierter Freizeichenton (RTP Stream) wurde bei einem ausgehenden Anruf nicht bei dem Anrufer signalisiert, da der Voice Call Manager nur den Port 5060 beachtete, statt den aktuellen Port mit der Session zum Provider.
  Wurde der ausgehende Anruf von einem ISDN- oder Analog-Teilnehmer initiiert, konnte der Freizeichenton nicht an den Anrufer signalisiert werden, da der Voice Call Manager zur Signalisierung auf ‚Local Ringtones' wechselte. Anschließend wurde die Meldung PROGRESS an den Teilnehmer versendet, wodurch die Signalisierung des Freizeichentons abgebrochen wurde.
  Die Meldung PROGRESS wird jetzt zuerst an den Teilnehmer versendet und danach der Freizeichenton signalisiert.

LCOS-Änderungen 10.40.0142 RC2

Neue Features

Allgemein

- Ab LCOS 10.40 RC2 wird der LANCOM vRouter um die Funktionen der LANCOM High Availability Clustering Option sowie der LANCOM Public Spot PMS Accounting Plus Option erweitert.
  HA Clustering gilt für alle LANCOM vRouter >= LANCOM vRouter 500
  PMS Accounting Plus gilt für alle LANCOM vRouter
  Kunden, die bereits einen LANCOM vRouter gekauft haben, können sich bei Bedarf über den LANCOM Support eine Ersatzlizenz generieren lassen.
- Unterstützung von MLD-Snooping
- Im SLA-Monitor können jetzt auch DSCP-Tags gesetzt werden.
- Die Cache-Zeit für die Verwendung von DNS-Objekten in der Firewall ist jetzt konfigurierbar.
- Das Hauptgerätepasswort und die Passwörter weiterer Administratoren können mittels der Hash-Verfahren SHA-256 und SHA-512 gespeichert werden.
- Die CRL-Prüfung ist jetzt pro IKEv2-Gegenstelle schaltbar.

Korrekturen / Anpassungen

Allgemein

- Beim LANCOM 883+ VoIP fehlte die Möglichkeit, den AiRISTA Flow Blink-Modus zu konfigurieren (/Setup/Wlan/Blink-Mode/). In der Folge konnte ein Gerät nicht in die LANCOM Management Cloud übernommen werden und es kam zu Fehlermeldungen nach einer Konfigurationsänderung.
- Beim vRouter funktionierte ein Portforwarding nicht, wenn ein Map-Port verwendet wurde, welcher ungleich dem angegebenen Port war.
- Auf einem vRouter konnten bei einem Portforwarding für PPTP die GRE-Pakete nicht der PPTP-Session zugeordnet werden. In der Folge wurden die GRE-Pakete nicht weitergeleitet und die PPTP-Verbindung funktionierte nicht.
- Wurde auf einem Router mit aktiver VPN-Verbindung auf dem der Versand von SNMP-Traps an einen per VPN-Verbindung erreichbaren Empfänger eingerichtet war, ein Firmware-Update auf eine LCOS-Version größer 10.12 durchgeführt, führte dies zu drei unvermittelten Neustarts des Routers. Im Anschluss wurde die alte Firmware wieder aktiviert. Eine Verwendung der aktuellen Firmware war dadurch nicht möglich.
- Bei DHCPoE-Verbindungen (nur IPv4) kam es nach der Erneuerung der IP-Parameter durch den Provider zu einem Neu-Aufbau der Default-Route und somit zu einem Abbruch aller Sessions. Dies konnte bei bestimmten Anschlüssen zu einem regelmäßigen Abbruch aller Verbindungen führen.
  Die Default-Route wird jetzt nur dann neu aufgebaut, wenn auch das Gateway geändert wurde.

- DNS-Ziele in der Firewall können u.a. dazu verwendet werden, um den Zugriff auf eine bestimmte Webseite zu unterbinden.
  Da Endgeräte über einen eigenen DNS-Cache verfügen und dieser die Adressen länger nachhielt als der Router, war ein Zugriff auf die Webseite häufig trotzdem möglich.
  Es ist jetzt möglich, eine Minimal-Zeit anzugeben, über die der Router DNS-Einträge nachhält. Der Standard-Wert beträgt 180 Sekunden.
- Werden IP-Netzwerke durch Zuweisung unterschiedlicher Schnittstellen-Tags ungleich 0 voneinander getrennt, kann die Kommunikation zwischen den beiden Netzwerken nur durch Erstellen einer entsprechenden Firewall-Regel erfolgen.
  Trotz passender Firewall-Regel wurde bei einem Zugriffsversuch von einem Netzwerkteilnehmer in einem der Netzwerke auf eine Ressource in einem der anderen Netzwerke per DNS der DNS-Name nicht aufgelöst. Dadurch war der Zugriff auf die Ressource nicht möglich.
- Nach der Konfiguration einer Internet-Verbindung auf einem im Werkszustand befindlichen LANCOM Router, konnte es vorkommen, dass DNS-Anfragen auf der funktionsfähigen Internet-Verbindung nicht beantwortet wurden.
- Beim Hairpin-NAT wurde eine rücklaufende Session von der Firewall des LANCOM Routers geblockt, wenn die Firewall eine ‚Deny-All'-Regel enthielt und zudem eine ‚Allow'-Regel für das Port-Forwarding als Quelle anstatt des Werts ‚Anyhost' den Namen der Internet-Gegenstelle verwendete.
- Aufgrund einer nicht berücksichtigten Port-Member-Liste konnte es vorkommen, dass der LANCOM Router unvermittelt neu startete, wenn ein T-Entertain-Receiver an diesen angeschlossen wurde.

VPN

- Eine IKEv2-VPN-Verbindung, bei welcher der EdDSA-Algorithmus (Edwards-Curve Digital Signature Algorithm) verwendet wurde, konnte aufgrund eines fehlerhaften Standard-Wertes während der Aushandlung der Security Associations (SAs) nicht aufgebaut werden.
- Im HSVPN-Profil in der Routing-Tag-Liste konnte per WEBconfig ein Minuszeichen gesetzt werden, obwohl dies nicht in der Liste der erlaubten Zeichen enthalten war.

WLAN

- Auf der WEBconfig-Oberfläche eines LANCOM LN-1700UE wurde ein Spectral Scan mit der Fehlermeldung ‚Data Connection Closed!' abgebrochen.
- Wurde auf LANCOM Access Points nach einem Skript-Rollout über einen WLAN-Controller der Befehl ‚show script' (Prüfung des Rollouts) per Kommandozeile eingegeben, kam es zu einem unvermittelten Neustart des Gerätes.

VoIP

- In Szenarien mit aktivem SIP-ALG kam es bei eingehenden Telefonaten dazu, dass in beide Richtungen keine Sprachdaten übertragen wurden.
- Ein VoIP-Telefon konnte sich bei Verwendung des SIP-ALG nicht an einer über eine VPN-Verbindung erreichbaren VoIP-TK-Anlage registrieren, da beim Versenden des Registrierungs-Paketes über die VPN-Verbindung der Quell-Port des VoIP-Telefons auf 0 anstatt auf 5060 gesetzt wurde.

- Wenn die Gegenseite einer VoIP-Telefonverbindung ein Re-INVITE an den LANCOM Router sendete, beantwortete der Router dieses mit einem INVITE, in welchem ein ‚Require: timer' mitgesendet wurde. Dieses INVITE wurde aufgrund des ‚Require: timer' vom Provider jedoch mit ‚BAD EXTENSION' abgelehnt. In der Folge wurde der Anruf beendet.
- In einem Szenario mit einer Netphone-/Swyx-TK-Anlage kam es bei einem eingehenden Anruf an einen SIP-Teilnehmer mit anschließender Weiterleitung an einen weiteren SIP-Teilnehmer zu einem Abbruch des Telefonats nach 15 Sekunden. Die Ursache war, dass der LANCOM Router auf die Meldung ‚200 OK' des Providers nicht mit der Meldung ‚ACK' antwortete und der Provider das Gespräch daher terminierte.
- Wenn bei einem ausgehenden Telefonat während der ‚Early Media Phase' von der Gegenseite die Meldung ‚180 Ringing' ohne SDP-Nachricht empfangen wurde, generierte der LANCOM Router keinen Dienst-Ton. Dies führte dazu, dass es bei dem anrufenden Teilnehmer nicht klingelte. Weiterhin konnte es vorkommen, dass keine Sprachdaten übertragen wurden und somit kein Telefonat möglich war.

LCOS-Änderungen 10.40.0103 RC1

Neue Features

Allgemein

- Neues Design für WEBconfig
- Syslog-Meldungen beim Firmwarewechsel sowie Firmware-Info beim Booten
- Für IPv6-WAN-Zugänge wird nun der DHCPv6-Client auch gestartet, wenn zuvor keine Router Advertisements empfangen wurden.
- Für die Zero-Touch-Inbetriebnahme an BNG-Anschlüssen der Deutschen Telekom wurde eine entsprechende Internet-Gegenstelle in die Standardkonfiguration von DSL-Routern aufgenommen.
- In der Standardkonfiguration muss nun bei der ersten Konsolen-Anmeldung ein Hauptgerätepasswort vergeben werden.
- Unterstützung von WAN-Verbindungen, denen providerseitig nur eine DHCPv4-Adresse mit /32-Maske zugewiesen wird
- Bei Erreichen von 80% eines konfigurierten Volumenbudgets erfolgt nun eine Information per E-Mail und/oder Syslog.
- Für QoS können nun WAN-Bandbreiten > 1 GBit/s konfiguriert werden.
- Unterstützung für High Availability Clustering im vRouter ab der Lizenzstufe „vRouter 500"
- Unterstützung für TLS 1.3 Client-Modus
- Zu sendende SNMP-Traps lassen sich nun filtern.
- Zu sendende Syslog-Meldungen lassen sich nun filtern.
- Für den Alive-Test ist nun eine Absende-Adresse konfigurierbar.
- Das RADIUS-Dictionary kann nun durch benutzerdefinierte Attribute erweitert werden.

Routing

- Unterstützung für Multicast-Routing
- Unterstützung für IGMP- und MLD-Proxy
- Unterstützung für PIM (Protocol Independent Multicast)
- Gegenstellen können nun bei Bedarf auch ohne vorhandene Route in der Routing-Tabelle aufgebaut werden.
- Der DHCP-Client unterstützt jetzt die Option 121 (Classless Static Route) nach RFC 3442.
- Der BGP-Connection-Retry-Timer ist nun konfigurierbar.
- Das Verhalten beim Propagieren der Default-Route im BGP kann jetzt konfiguriert werden.
- BGP speichert jetzt eine Historie über gesendete Präfixe.
- Die IPv4-Firewall unterstützt nunmehr keine MAC-Adressen als Ziel. Bestehende Konfigurationen funktionieren weiterhin.
- Die zeitgesteuerte Default-Route ist entfallen.
- Für statische IPv4- und IPv6-Routen kann nun die administrative Distanz konfiguriert werden.
- Unterstützung für NetFlow/IPFIX
- Die administrative Distanz bei OSPF ist jetzt konfigurierbar.
- Für die Route-Redistribution via LISP und OSPF kann eine Präfix-Filterliste konfiguriert werden.
- Die Zeile „DMZ“ wurde aus einigen Tabellen als Vorbelegung entfernt.
- Der TFTP-Operating-Schalter beherrscht jetzt auch den Modus „Nur Sysinfo“.
- Die Skalierbarkeit des IPv4-Routers bei vielen Routen wurde deutlich verbessert.
- Überträgt der Provider die tatsächliche Layer-3-Bandbreite als zusätzliche Information im PPP, so wird diese im QoS verwendet.

VPN

- Unterstützung für LANCOM High Scalability VPN (HSVPN)
- Unterstützung für IKEv2 EAP
- Unterstützung für ChaCha20-Poly1305 für IKEv2
- Unterstützung für EdDSA für IKEv2
- Unterstützung für Digital Signature mit ECDSA nach RFC 7427
- Unterstützung für Curve25519 und Curve448 für IKEv2
- Ein VPN-Loadbalancer kann dynamisch durch RADIUS erzeugt werden.
- Das Anfragen einer Adresse im IKEv2-Config-Mode ist jetzt schaltbar.
- Alternative Gateways können nun gruppiert und priorisiert werden.
- Entfall von IPCOMP für IKEv1
- Entfall von AH für IPsec

WLAN

- Unterstützung für OCSP im RADIUS-Server im Zusammenhang mit EAP(-TLS)
- WLAN-SSIDs können anhand von Zeitplänen ein- und ausgeschaltet werden.
- Für Public Spot kann nun ein benutzerdefiniertes Branding-Logo („powered by LANCOM“) auf der Login-Seite verwendet werden.

- Unterstützung für die LANCOM Publlic Spot PMS Accounting Plus-Option im vRouter
- Für die Public Spot-Anmeldeseite wird nun immer HTTPS verwendet, wenn als Login-Seiten-Protokoll „HTTPS“ ausgewählt ist. Zuvor wurden nur die eigentlichen Anmeldedaten und die Status-Seite über HTTPS übertragen.
- Für WLAN-Clients kann ein Schwellwert definiert werden, bei dessen Unterschreitung ein Client disassoziiert wird.
- VLAN-Gruppenschlüssel werden nun automatisch vergeben.

VoIP

- Passwörter für SIP-Leitungen dürfen nun bis zu 64 Zeichen lang sein.
- Unterstützung für „Telekom Company Flex“-Zugänge.
- Das Format der „Connected Number“ ist konfigurierbar
- Unterstützung Early Media
- Rufe können dynamisch auf verschiedene SIP-Leitungen verteilt werden
- Die maximale Anzahl von parallelen Gesprächen für eine SIP-Leitung ist konfigurierbar

WLC

- „Unbekannte gesehene Clients“ werden in der Standardkonfiguration nicht mehr an den WLC gemeldet.
- Die Client-Bandbreitenbegrenzung ist nun über den WLC konfigurierbar.

Korrekturen / Anpassungen

Allgemein

- Wenn ein Zertifikat via SCEP in einen VPN-Container des LANCOM Routers geladen wurde und es das gleiche Subject aufwies wie ein Zertifikat, welches sich bereits in einem VPN-Contrainer befand, wurde das Zertifikat mit einem Unknown-Status versehen und konnte nicht ausgerollt werden.
- Wenn bei Geräten des Typs LANCOM 1780EW-4G+, LANCOM 1793VA-4G oder LANCOM 1790-4G im Mobilfunk-Profil die Übertragungsarten „UMTS(3G)+GPRS(2G)“ oder „GPRS(2G)“ eingestellt wurden, verwendete das Gerät immer LTE(4G), weil das verbaute Mobilfunkmodul dieser Geräte die Übertragungsart GPRS(2G) nicht unterstützt. Das Gerät baut nun eine Verbindung zum 3G-Netz auf.
- Über GPS kann neben der Positionsbestimmung auch der Bezug der Uhrzeit erfolgen. LTE-Router mit dem LTE-Modul MC7710 gaben als Uhrzeit „2001-01-01 00:00:00“ + Betriebszeit des Routers aus. Die Zeit-Synchronisation per GPS wird nun deaktiviert, wenn offensichtlich falsche Werte empfangen werden.
  Betroffen waren folgende Geräte:
  - 1780EW-4G Hardware Rel. B und C (teilweise)
  - 1781VA-4G Hardware Rel. B und C (teilweise)
  - 1781-4G
  - 1781A-4G (teilweise)
- Wurde per Rollout-Wizard ein Skript auf einen Router ausgerollt, welches einen einzelnen Wert in einer Tabellen-Zeile setzte, kam es zu einem unvermittelten Neustart des Routers.

VoIP

- Der Voice Call Manager unterstützte keine multiplen Dialoge in der Early Media Phase. Bei Telefonaten mit multiplen Dialogen (etwa bei Verwendung eines Call-Routings über einen Telefon-Dienst) führte dies dazu, dass beim Zustandekommen des Telefonats keine Sprachdaten übertragen wurden.
- In einem Szenario mit einer per Gateway-Leitung angebundenen SIP-TK-Anlage wurde bei einem eingehenden Telefonat vom LANCOM Router die Session-ID in den SDP-Informationen nicht hochgezählt. Dies führte dazu, dass das Telefonat bei Annahme des Gesprächs abgebaut wurde.
- In der Call-Routing-Tabelle war die Anzahl der möglichen Einträge auf maximal 128 begrenzt. Diese Begrenzung wurde aufgehoben.
- Bei Telekom-VoIP-Anschlüssen konnte es vorkommen, dass bei einem per SIP-Client initiierten Festnetz-Anruf kein „Klingeln"-Signal auf der Leitung ausgegeben wurde, da der Provider ein „Ringing" ohne Session Description Protocol (SDP) sendete. In der Folge verlief der Rufaufbau bis zur Rufannahme ohne Ton-Signalisierung.
- Auf Geräten der 1783x-Serie wurden im WEBconfig bei einem Eintrag für einen analogen Benutzer alle analogen- und Wähl-Schnittstellen als ausgewählt angezeigt, wenn ein Benutzereintrag lediglich mit der analogen- und Wähl-Schnittstelle 2 abgespeichert wurde.

6. 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.