Release Notes

LCOS
9.24 SU13

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 9.24 SU13 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Updates unbedingt die Hinweise im Kapitel 5 „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 9.24

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 9.24

→ LANCOM 1711+ VPN
→ LANCOM 1721+ VPN
→ LANCOM 1722 VoIP
→ LANCOM 1723 VoIP
→ LANCOM 1724 VoIP
→ LANCOM 1811n Wireless
→ LANCOM 1821+ Wireless ADSL
→ LANCOM 3850 UMTS
→ LANCOM 800+
→ LANCOM DSL/I-10+
→ LANCOM L-315agn dual Wireless
→ LANCOM OAC-54-1 Wireless
→ LANCOM OAP-310agn Wireless
→ LANCOM OAP-54 Wireless
→ LANCOM WLC-4006
→ LANCOM WLC-4025
→ LANCOM XAC-40-1
→ Swyx 1722 VoIP
→ Swyx 1723 VoIP
→ Swyx 1724 VoIP

4. Historie LCOS 9.24

LCOS-Änderungen 9.24.0475 SU13

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 9.24.0474 SU12

Korrekturen / Anpassungen

Allgemein

→ Es wurde ein potentiell sicherheitsrelevantes Problem auf LANCOM Routern in Verbindung mit IPv6 behoben.
Dieses kann auftreten, wenn IPv6-Netze über IPSec (IKEv1 oder IKEv2) verbunden werden und gleichzeitig eine IPv6-Internet-Verbindung verwendet wird.
In diesem Fall wird eine Aktualisierung auf die aktuelle LCOS-Version dringend empfohlen.
Der Fehler ist in den folgenden LCOS-Versionen behoben:

- LCOS 10.32 SU3
- LCOS 10.20 SU9
- LCOS 10.12 SU14
- LCOS 9.24 SU12
- LCOS 9.00 SU8
- LCOS 8.84 SU11

WLAN

→ Wechselte ein Client auf einem Dual-Radio Access Point mit zwei AC-Modulen von einem Modul auf das andere, so konnte es sporadisch zu dem Effekt kommen, dass der Access Point dem Client keine eindeutige Association ID vergab und für den Client keine Datenübertragung möglich war.

→ Wenn eine Public Spot-Anmeldung per HTTPS (TSLv1.3) durchgeführt wurde, erhielt der Benutzer anstatt einer Login-Seite eine Information des Browsers mit einer „Blockieren“-Meldung. In der Folge konnte sich ein Benutzer nicht am Public Spot anmelden.

VoIP

→ Es wurde ein VoIP-Problem behoben, bei dem in bestimmten Konstellationen mit analogen Telefonen einseitige Sprachverbindungen oder keine Verbindung zustande kommen konnte. Für folgende Geräte wird das Update bereitgestellt:

- LANCOM 1783VA, 1783VAW, 1783VA-4G
- LANCOM 1793VA, 1793VAW, 1793VA-4G
- LANCOM 1906VA, 1906VA-4G
- LANCOM 883 VoIP

LCOS Änderungen 9.24.0472 RU11

Korrekturen / Anpassungen

Allgemein

→ Der SCEP-Client legte beim erstmaligen Bezug eines Geräte-Zertifikates das zuerst erhaltene CA-Zertifikat direkt in den definierten VPN-Container. Dies führte zu einem unvollständigen VPN-Container, welcher vom VPN nicht genutzt werden konnte.
Das CA-Zertifikat wird nun in einem temporären Container abgelegt. Wenn alle Elemente des Containers vorliegen, schreibt der SCEP-Client die Datein in den definierten Container.

→ Der SCEP-Client nutzte für einen Erstbezug eines Zertifkats fälscherlicherweise den Befehl „GetNextCACert“ anstelle des Befehls „GetCACert“. Dies führte dazu, dass die Zertifizierungsstelle den Request mit den HTTP-Fehler „400 Bad Request“ beantwortete.

→ Bei der Verwendung von WLAN-Routern oder Access Points, die ein 802.11n-WLAN-Modul verwenden, kam es zu Verbindungsabbrüchen im 2,4 GHz Band, wenn ein im Powersave-Modus befindlicher WLAN-Client bei der Frame-Aggregation kleinere Reordering-Frames zuließ, als normalerweise üblich (z.B. 8 statt 64 Pakete). Davon waren z.B. Amazon ECHO-Geräte betroffen.

→ Bei gleichzeitiger Verwendung von eBGP und iBGP konnte es dazu kommen, dass Routen mit statischen Präfixes für eBGP zurückgezogen wurden. In der Folge war eine Kommunikation zwischen verschiedenen AS (autonomous system) nicht mehr möglich.

→ Das Abfrage-Intervall für den Bezug von Zertifikaten über den SCEP-Client in dem Pfad /Setup/Certificates/SCEP-Client/Check-Pending-Requests-Interval wurde ignoriert und stattdessen ein fester Wert von 60 Sekunden verwendet. Es wird jetzt wieder der hinterlegte Wert herangezogen.

→ In zertifikatsbasierten Szenarien (VPN und WLC), in welchen der interne SCEP-Client des LANCOM Routers zur Verteilung der Zertifikate verwendet wurde, erneuerte der SCEP-Client auslaufende RA-Zertifikate nicht automatisch. In der Folge konnten z.B. zertifikatsbasierte VPN-Verbindungen nicht mehr aufgebaut werden bzw. Access Points, welche von einem WLC verwaltet wurden, konnten keine Verbindung mehr zu diesem aufbauen.
Weitere Informationen zu diesem Verhalten können Sie in der LANCOM Support Knowledge Base nachlesen.

Aufgrund eines Fehlers bei der Gültigkeitsprüfung konnte das Geräte-Zertifikat bei Verwendung der Funktion RA-Auto-Approve nicht erneuert werden. Dies führte in WLC- und VPN-Szenarien dazu, dass die Zertifikate nicht bezogen werden konnten. Weitere Informationen zu diesem Verhalten können Sie in der LANCOM Support Knowledge Base nachlesen.

Bei einer Zertifikats-Anfrage über den SCEP-Client konnte es bei externen Zertifizierungsstellen (z.B. Windows CA) dazu kommen, dass das Zertifikat nicht angenommen werden konnte, da der „mime type“ falsch war. Das Zertifikat wird jetzt direkt überprüft ohne den „mime type“ zu beachten.

LCOS Änderungen 9.24.0411 PR

Korrekturen / Anpassungen

Allgemein

→ Wenn ein Provider während der LTE-Attach-Phase Anmeldedaten (Benutzername und Passwort) forderte, wählte der LANCOM Router falsche Anmeldedaten (von einer anderen Gegenstelle) aus, wenn in diesem Moment keine andere beliebige Internet- oder IPSec-Verbindung aufgebaut war.

→ In SNMPv3 wurde bei der Abfrage des LLDP-Pfades eine Korrektur in der Index-Bildung vorgenommen.

→ In seltenen Fällen konnte es zu einer Falschberechnung einer UDP Checksumme für die Maskierung (NAT) kommen.

→ Routen, bei denen die Netzadresse in allen vier Oktetts dezimal komplett ausgefüllt war (z.B.

→ 192.168.100.100/30), wurden per BGP entweder gar nicht oder falsch (z.B. als 0.0.0.0/26) propagiert.

→ Die OpenSSL Library wurde auf die Version 1.0.2o aktualisiert.

→ In der Application-Firewall wurde eine konfigurierte Aktion bereits während der Detect-Phase ausgeführt. Das Ausführen einer Aktion erfolgt nun erst, nachdem das Protokoll bestätigt wurde.

→ Eine xDSL-Verbindung wurde nicht sofort abgebaut, wenn die dazugehörige DSL-Gegenstelle per Skript aus der Konfiguration gelöst wurde

VPN

→ Durch Optimierungen im GRE-Protokoll wurde die Routing-Performance von GRE-Tunneln (sowohlLAN-LAN als auch LAN-WAN) um etwa 15 % gesteigert.

VoIP

→ Es konnte zu einem unvermittelten Neustart des Routers kommen, wenn bei einem über eine SIPTrunk-Leitung geführten Telefonat weitere Ziffern nachgewählt wurden.

→ Im Menü „Voice Call Manager → Erweitert → Quality of Service → Abgehende Pakete bevorzugen“ war nach einem Werksreset der Wert „Reduktion der PMTU & Fragmentierung“ als Standard eingestellt, obwohl hier der eigentliche Standardwert „Reduktion der PMTU“ eingestellt sein sollte.

→ Eine Fax-Übertragung über T.38 konnte scheitern, wenn die RTP-Fax-Pakete kleiner als RTP-Audio-Pakete waren, da eine Prüfung auf Paket-Länge ausgeführt wurde. Die Prüfung wird nicht mehr ausgeführt, da RTP-Fax-Pakete kleiner sein können als RTP-Audio-Pakete.

LCOS Änderungen 9.24.0358 PR

Korrekturen / Anpassungen

Allgemein

→ In manchen Fällen wurden Routen mit der Einstellung „Sticky für RIP“ nicht korrekt über das RIPProtokoll
→ propagiert.
→ Der SNMP-Zugriff auf einen LANCOM Router war über eine WAN-Schnittstelle nicht mehr möglich, wenn in den Zugriffsrechten der WAN-Schnittstelle das Recht „Nur lesen“ für SNMP konfiguriert war.
→ Änderungen an der VLAN-Provider-Liste im Pfad /Setup/WAN/VLANs/Provider-List wurden erst nach einem Neustart des Routers wirksam.
→ Es konnte sporadisch zu einem unvermittelten Neustart des Gerätes kommen, wenn der Befehl „do/Status/Modem-Mobile/Scan-Networks“ (der Befehl ermittelt den WWAN-Provider mit der besten Qualität) per Cron-Job ausgeführt wurde.

VPN

→ Es wurden keine Daten durch den VPN-Tunnel übertragen, wenn eine IKEv2-Verbindung über den IPSec-over-HTTPS-Modus aufgebaut wurde. Betroffen waren IKEv2-Verbindungen zwischen zwei LANCOM Routern und ebenfalls IKEv2-Verbindungen zwischen Advanced VPN Client und einem LANCOM Router.

VoIP

→ In der URI des Route-Headers eines SIP-Pakets wurde das “SIP“ großgeschrieben, was nicht RFC-konform ist und dazu führen konnte, dass bestehende Rufe nach 30 Sekunden abgebaut wurden.
→ Der LANCOM Router übermittelte auf dem ISDN die Rufnummer aus dem Feld „P-Asserted-Identity“ als Calling Number mit dem Merkmal „screening indicator : user provided, not screened“. Dies führte dazu, dass die Rufnummern in einigen Telefonanlagen als „ungeprüft, unseriös“ markiert wurden.

LCOS Änderungen 9.24.0334 SU9

Korrekturen / Anpassungen

Security Update für LANCOM Router, Gateways, Access Points und WLAN Controller

→ Das Update behebt eine sicherheitsrelevante Schwachstelle in den Management-Funktionen.
Potentiell betroffen sind alle Geräte, die mit folgenden Firmware-Versionen laufen:
LCOS 10.12 REL, SU1, RU2
LCOS 10.10 RU2, 10.10.0165 PR, 10.10 RU4
LCOS 9.24 RU6, SU7, RU8
Für diese Geräte wird das Update empfohlen. Alle anderen Versionen sind nicht betroffen.

LCOS Änderungen 9.24.0330 RU8

Korrekturen / Anpassungen

Allgemein

→ Es wurden Pakete übertragen, welche durch eine Firewall-Regel zurückgewiesen werden sollten, wenn in der Firewall zwei QoS-Regeln mit jeweils aktivierter Verlinkung („Weitere Regeln beachten, nachdem diese Regel zutrifft“) aktiv waren und die Pakete auf eine dieser QoS-Regeln zutrafen.

→ Unter /Setup/DNS/DNS-Destinations konnten keine zwei Server als Ziel eingetragen werden, wenn einer oder beide mit dem ‚@‘-Zeichen erweitert wurden. Mit dem ‚@‘-Zeichen kann ein Routing-Tag spezifiziert werden.

→ Es konnten keine Objekte in der Firewall (LCOS-Menübaum: /Setup/IP-Router/Firewall/Objects; LANconfig: Firewall/QoS > IPv4-Regeln > Stations-Objekte) angelegt werden, welche das ‚@‘-Zeichen enthielten, obwohl der erlaubte Zeichensatz das ‚@‘-Zeichen beinhaltete.

→ Wenn das „iperf“-Kommando in der Komandozeile des LANCOM unvollständig oder abgekürzt eingegeben wurde (z.B. „iper“ statt „iperf“), startete der iperf-Server mit einer Warnmeldung.

VPN

→ Es war nicht möglich, mehrere Dynamic-VPN-Aushandlungen gleichzeitig auszuführen. Dies führte dazu, dass die zugehörigen VPN-Tunnel nicht aufgebaut werden konnten.

VoIP

→ Wenn eine VoIP-Konfiguration über den Setup-Assistenten in das Gerät geschrieben wurde und in diesem Moment über die noch bestehende VoIP-Konfiguration ein Ruf vermittelt wurde, konnte es zu einem unerwarteten Neustart des Gerätes kommen.

→ Der Voice Call Manager wertete nicht die Allow-Header von empfangenen SIP-Paketen aus, sondern fügte immer eine eigene feste Allow-Liste ein, wenn er einen Ruf vermittelte.

LCOS Änderungen 9.24.0322 SU7

Korrekturen / Anpassungen

WLAN

→ Es wurde eine Sicherheitslücke im WPA2-Verfahren (KRACK-Attacke) im Zusammenhang mit der Nutzung von 802.11r (Fast-Roaming) im AP-Betrieb (Basisstation) behoben:
CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and
reinstalling the pairwise key while processing it
Bitte informieren Sie sich zudem beim jeweiligen Hersteller über die Verfügbarkeit von Updates für Ihre WLAN-Clients. Auch diese Geräte müssen aktualisiert werden.

→ Es wurde eine Sicherheitslücke im WPA2-Verfahren (KRACK-Attacke) im Zusammenhang mit der Nutzung des WLAN-Client-Modus / WLAN-Station-Mode mit 802.11ac-WLAN-Modulen, sowie bei Benutzung von Punkt-zu-Punkt-Strecken mit 802.11ac- und 802.11a/b/g/n-WLAN-Modulen behoben:
CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
CVE-2017-13080: reinstallation of the group key in the Group Key handshake
Der mit 802.11a/b/g/n-WLAN-Modulen betriebene WLAN-Client-Modus / WLAN-Station-Mode ist nicht betroffen.

Hinweis:

Von den folgenden WPA2-Sicherheitslücken (KRACK-Attacke) ist das LCOS nicht betroffen:

→ CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
→ CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
→ CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
→ CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
→ CVE-2017-13078: reinstallation of the group key in the Four-way handshake

→ CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

→ CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

LCOS Änderungen 9.24.0314 RU6

Korrekturen / Anpassungen

Allgemein

→ Proxy-ARP für die Kommunikation zwischen identischen, vom LANCOM verwalteten IP-Netzwerken, wurde nicht ausgeführt.

→ Bei Verwendung eines Backup-RADIUS Servers zur Geräte-Authentifizierung wurde das Login zuerst auf dem Backup-Server statt auf dem primären RADIUS-Server geprüft.

→ Bei der Verwendung des „sleep“-Befehls wurden als Stunden-Einheit nur Werte zwischen 5 und 7 Stunden akzeptiert. Bei der Verwendung von Sekunden als Einheit waren nur Werte bis 900 Sekunden möglich.

→ Wenn vom einen Server in der DMZ zu große Pakete (größer als die MTU der Ziel-Gegenstelle) an LANCOM Router gesendet wurden, in denen das DF-Bit (don‘t fragment) gesetzt war, so sendete der LANCOM Router keine ICMP-Fehlermeldung mit der Nachricht „fragmentation needed...“ an den Sender der Pakete und verwarf diese.

→ Eine xDSL-Verbindung wurde nicht sofort abgebaut, wenn die dazugehörige DSL-Gegenstelle per Script aus der Konfiguration gelöst wurde.

→ Es kam zu einem Script Error, wenn der Befehl „Loadfile“ über ein Skript aufgerufen wurde. Der Befehl „Loadfile“ wurde aber dennoch ausgeführt.

→ Es konnte zu einem unvermittelten Neustart des Gerätes nach Aufruf des benutzerdefinierten Rollout-Assistenten kommen, wenn im benutzerdefinierten Rollout-Assistent für eine Auswahl-Liste mehr Werte (item_value) als Text (item_text) definiert waren.

→ Wenn ein BGP-Router ein bestimmtes Präfix verteilte, welches der Nachbar auch aus einer anderen Quelle gelernt hatte (und diese somit auch propagierte), fand kein Route-Revoke für dieses Präfix an diesen BGP-Nachbarn statt.

→ In einem VRRP Loadbalancing Szenario mit RIP wurden ICMP Redirects mit der Quell-IP-Adresse des ARF-Kontextes und nicht mit der VRRP-IP-Adresse versendet.

VPN

→ Es wurden weitere IPSec-Regeln generiert, wenn für eine VPN-Gegenstelle ausschließlich eine übergeordnete IPSec-Regel, zum Beispiel ANY-to-ANY, definiert war, aber auch für diese VPNGegenstelle ein oder mehrere N:N-NAT-Einträge hinterlegt waren, welche die übergeordnete IPSec-Regel einschloss.

→ Wenn in der Konfiguration für eine IKEv2-Client-Verbindung kein IPv4-Adressen-Pool angelegt wurde, so erhielt der IKEv2-Client, welchem über den IKE-Config-Mode vom LANCOM Router eine IP-Adresse zugewiesen wurde, keinen DNS-Server. Der LANCOM Router weist dem IKEv2-Client als DNS-Server die eigene IP-Adresse zu, wenn kein IPv4-Adressen-Pool angelegt ist.

→ Wenn eine maskierte IKEv2 VPN-Verbindung zwischen zwei LANCOM Routern aufgebaut wurde, bei welcher auf einer Seite eine DMZ transparent (Maskierungs-Einstellung „nur Intranet“) erreichbar sein sollte, so wurde auch die DMZ maskiert.

→ Eine IKEv2-Verbindung mit einen Digital-Signature-Profil „RSASSA-PSS mit SHA-384 und SHA-512“ konnte nicht aufgebaut werden.

→ Wenn auf einem LANCOM Router ausschließlich Default-Routen mit einem Routing-Tag ungleich 0 definiert waren, so konnten IKEv2-Verbindungen nicht aufgebaut werden, wenn der IKEv2-Peer nicht anhand der IP-Adresse erkannt wurde.

WLAN

→ Wenn im Menü Public-Spot > Assistent > Bandbreitenprofile entsprechende Profile angelegt waren, wurden die Werte in der späteren Darstellung im Assistenten und auf dem Voucher vertauscht dargestellt.

→ Auf der Login-Seite des Public-Spot-Gateways konnten die Seite mit den Nutzungsbedingungen von Apple-Clients nicht aufgerufen werden, wenn das Authentifizierungsverfahren für den Public Spot auf “Anmeldedaten werden über E-Mail / SMS versendet” stand.

→ Bei einem LANCOM WLAN-Controller wurde nach Durchführung einer Funkfeldoptimierung im LANmonitor ein negativer Wert für verwaltete Access Points angezeigt.

→ Wenn in einem Public-Spot-Szenario auf einem Router mit WLAN-Modul der Public Spot betrieben wurde und im lokalen Netz ein weiterer Access Point angeschlossen war, welcher ebenfalls die Public Spot-SSID ausgestrahlte, wurde der Benutzereintrag beim Roaming vom WLAN-Router auf den Access Point aus der Auto-Re-Login-Tabelle gelöscht. Dies führte dazu, dass ein erneutes Einloggen am Public Spot erforderlich war.

VoIP

→ Sollte eine Rufgruppe als Backup-Leitung, z.B. für eine Verbindung zu einer TK-Anlage, verwendet werden, so funktionierte dieser Eintrag nicht.

→ Wenn die Einrichtung eines All-IP Anschlusses im WEBconfig mit dem Setup-Assistent “Voice-over-IP / All-IP einrichten” vorgenommen wurde, blieb die eingerichtete ISDN-Schnittstelle nach Durchlauf des Assistenten im Schaltzustand “Aus”.

→ Es konnte sporadisch eine einseitige Verständigung auftreten, wenn ein eingehender Ruf über eine SIPLeitung vom LANCOM VoIP-Router intern auf mehr als 2 Interfaces (ISDN- und Analog-Schnittstellen) signalisiert wurde.

→ Nachdem ein analoger Anruf beendet wurde, blieb dieser in seltenen Fällen in der Call Counter-Tabelle des LANCOM VoIP-Routers als Eintrag erhalten.

→ In einem Telefonat, welches zwischen einem LANCOM VoIP Router und einer Unify SIP-TK-Anlage aufgebaut war, kam es zu einer einseitigen Verständigung, wenn das Gespräch nach einem “HOLD” zurückgeholt wurde.

LCOS Änderungen 9.24.0261 RU5

Korrekturen / Anpassungen

Allgemein

→ Routen, die über eBGP empfangen wurden, wurden bei der Pfadauswahl bevorzugt. Die MED (Multi Exit Discriminator) wurde erst anschließend geprüft.

→ Wenn der LANCOM Router eine „ICMPv6 packet too big“-Nachricht für Pakete, die auf ein Ziel- Interface ohne globale Adresse geroutet werden sollten (z.B. VPN-Interfaces), versenden musste, wurde die Nachricht mit der Link-Lokalen-Adresse versendet.

→ Nachdem verwaltete LANCOM Access Points ein Profil von einem WLAN Controller erhalten haben, welcher als DHCP-Server konfiguriert ist, und bei welchem zudem eine Lease-Time konfiguriert ist, welche kleiner als die Standardeinstellung ist, waren die Access Points zwar unter der im Profil festgelegten IP-Adresse erreichbar, verloren diese aber nach einiger Zeit und verblieben in diesem Zustand.

→ Es konnte zu einem unvermittelten Neustart des Gerätes bei einem Zugriff via SSH kommen, wenn die SSH-Authentifizierung mit Hilfe eines Public Keys erfolgte, das Gerät diesen Public Key akzeptierte, der SSH-Client jedoch eine Signatur gesendet hatte, welche vom LANCOM Router über den Public Key nicht verifiziert werden konnte.

→ Der TFTP-Server im LANCOM Router konnte die Ports im Bereich von 8192 bis 16383 blockieren und gab diese erst nach einem Neustart des Gerätes wieder frei. In der Folge konnte es zu Problemen beim Port-Forwarding der genannten Ports kommen.

→ Der WEBconfig Setup-Wizard „Internet-Verbindung einrichten“ setzte bei Auswahl eines Ethernet-Interfaces unter „Setup/Interfaces/DSL“ auf dem ausgewählten DSL-Interface eine Downstream-Rate von 2176 KBit/s, eine Upstream-Rate von 2176 KBit/s und einen externen Overhead von 12 Byte, ohne dass dies definiert wurde.

→ Wenn bei einer bestehenden WWAN-Verbindung die Netz-Auswahl im Mobilfunk-Profil auf den Parameter „Nach Qualität“ eingestellt war und in der Kommandozeile ein Netzwerkscan mit dem Befehl „scan-networks -s“ oder im LANmonitor mit der Option „Verbindung trennen und bestes Netz auswählen“ ausgeführt wurde, verwendete das WWAN-Modul nicht das beste gefundene Netz, welches nach dem Scan im Profil hinterlegt wurde, sondern das Netz, welches zuletzt erfolgreich verwendet wurde.

VPN

→ Im IKE-Teil einer VPN-Verbindung wurde nach einer Konfigurationsänderung solange keine CRLPrüfung mehr durchgeführt, bis der CRL-Client die nächste CRL abholte.

→ Wenn eine IKEv2-Verbindung mit IKE-CFG Mode eingerichtet und die zu verwendende IPv4-Adresse in der IP-Parameter-Liste fest konfiguriert war, fragte der LANCOM Router beim Verbindungsaufbau nach einer IPv6-Adresse, obwohl IPv6 in der Konfiguration nicht aktiviert ist. Da der Partner keine IPv6-Adresse zuweisen konnte, wurde die VPN-Verbindung nicht aufgebaut.

→ Es konnte zu einem unvermittelten Neustart des Gerätes bei Nutzung des CRL-Clients kommen, wenn dieser die CRL-URLs nicht abrufen konnten, da z.B. der Server nicht aufgelöst oder erreicht werden konnte.

→ Wenn bei einer IKEv2-VPN-Verbindung ein Verbindungsabbau durch eine Seite initiiert wurde (z.B. nach einer Konfigurationsänderung), wurde die Phase 2 SA nur auf einer Seite (beim Initiator) abgebaut. Dies hatte zur Folge, dass ein erneuter Verbindungsaufbau für diese VPN-Verbindung scheiterte.

→ Bei einem simultanen Rekeying (beide Seiten starten zur gleichen Zeit eine Aushandlung von neuem Schlüsselmaterial) auf einer IKEv2-Verbindung wurden nach Abschluss beide neuen CHILD-SAs gelöscht, so dass keine Datenpakete mehr über die Verbindung transportiert wurden.

WLAN

→ Bei der Durchführung eines Spectral Scans wurde die Zeitachse im Wasserfall-Diagramm nicht angezeigt.

→ Ein LANCOM Access Point sendete den IAPP Handover Request an die falsche IP-Adresse, wenn ein als WLAN-Client konfigurierter LANCOM Access Point zu einem anderen Access Point wechselte.

→ Die Zähler „TX-Bytes“ und „RX-Bytes“ wurden nach einer Abmeldung nicht zeitnah zurückgesetzt, so dass, wenn ein Datenvolumen („Setup/Public-Spot-Modul/Traffic-Limit-Bytes“ oder „Public-Spot → Server → Zugriff ohne Anmeldung → Max. Datenvolumen) konfiguriert war und dieses über die Zähler ausgeschöpft war, eine sofort ausgeführte erneute Anmeldung nicht möglich war. Es existiert ab jetzt ein neuer Zähler mit Namen „Unauthenticated-Bytes“, welcher das verbrauchte Datenvolumen eines Public-Spot-Benutzers vor seiner Authentifizierung anzeigt.

→ Der Trigger zur Re-Initialisierung des SCEP-Clients konnte ins Leere laufen, wenn sich der Client gerade in der Initialisierung befand.

VoIP

→ Wurde über eine Konsolen-Sitzung der Analog-Port unter „Setup/Interfaces/Analog“ deaktiviert, konnte der Port über LANconfig unter „Voice Call Manager → Benutzer → Analog Schnittstellen“ nicht wieder aktiviert werden.

→ Abgehende Telefonate über den SIP-Provider M-net konnten nicht aufgebaut werden, da der Provider sowohl nach der Authentifizierung über ein „INVITE“ als auch nach einem „PRACK“ eine Authentifizierung fordert.

→ Wenn für einen Analog-Benutzer und für einen ISDN-Benutzer die gleiche Rufnummer im Voice Call Manager hinterlegt wurde, und das ISDN-Telefon physikalisch nicht mit dem LANCOM Router verbunden war, wurde keine „Besetzt“-Signalisierung an den SIP-Provider gemeldet, wenn ein Gespräch über das analoge Endgerät geführt wurde, und zeitgleich auf der Rufnummer ein Anruf einging.

→ Bei Telekom SIP-Trunk-Anschlüssen kam es zu Problemen bei der Faxübertragung, wenn versucht wurde, T.38 auszuhandeln. Scheiterte die T.38-Aushandlung, so erfolgte kein Rücksprung auf das G.711-Protokoll und die Fax-Übertragung wurde unterbrochen.

→ Wenn ein Anruf über eine ISDN-TK-Anlage erfolgte, die an der internen ISDN-Schnittstelle des LANCOM Routers angeschlossen ist und über eine konfigurierte Rufweiterleitung an externe Nummern verfügt,führte dies zu einer unidirektionalen Kommunikation, wenn der Ruf schließlich über den VCM per SIP zum Provider weitergeleitet wurde.

→ Eine SIP-Session, welche über eine Firewall-Regel mit einen Routing-Tag versehen wurde und dann durch den SIP-ALG gemanagt wurde, konnte nicht aufgebaut werden, da die Antwort-Pakete mit dem gleichen Tag (Quell-Tag) vom SIP-ALG versehen, und so vom IP-Router verworfen wurden.

LCOS Änderungen 9.24.0212 RU4

Korrekturen / Anpassungen

Allgemein

→ Lokale IPv6-Netzwerke können wieder untereinander kommunizieren, wenn eines dieser Netzwerke einer Bridge-Gruppe zugeordnet war (z.B. BRG-1), und das andere Netzwerk einem logischen Netzwerk (z.B. LAN-2).

→ Ein Gerät im unkonfigurierten Werkszustand kann im lokalen Netzwerk wieder über einen beliebigen DNS-Namen erreicht werden.

→ Wenn die Uhrzeit auf einem Gerät gesetzt wird (manuell oder per NTP-Server), werden auch die Millisekunden zurückgesetzt.

→ Auch bei Internet-Verbindungen über die Provider SWN oder Wilhelm-tel wird auf dem WAN-Interface eine IPv6-Adresse erzeugt.

→ Ein durch einen Client als NTP-Server angesprochenes Standby-Gerät in einem VRRP-Verbund baut bei aktiviertem NTP-Server-Dienst keine Internetverbindung mehr auf.

→ Bei einem Router, auf dem per WAN-RIP eingebunde Gegenstellen (z.B. L2TP oder PPTP) konfiguriert sind, führt eine beliebige Konfigurationsänderung nicht mehr dazu, dass Gegenstellen, die zu diesem Zeitpunkt keine aktive RIP-Route haben, getrennt werden.

→ Die Begrenzung des Datenverkehrs per Firewall-Regel mit dem Trigger „pro Station“ funktioniert wieder, wenn in der Konfiguration des LANCOM Gerätes ein logisches LAN-Interface (z.B. LAN-1) einer Bridge-Gruppe (z.B. BRG-1) zugeordnet, und in der IP-Netzwerk-Konfiguration explizit ein logisches LAN-Interface zugeordnet ist.

→ Das zweite logische EXT-Interface wurde in die MIB-2 aufgenommen.

→ Bei Geräten ohne Dual-SIM wird kein zweites logisches EXT-Interface im Status-Baum ausgegeben.

→ Dynamisch via eBGP, iBGP oder RIP gelernte Routen werden in der Fowarding Information Base (siehe auch LANCOM Knowledgebase) nur noch ihrem dazugehörigen Routing-Kontext (Routing-Tag) hinzugefügt.

→ Bei der IKEv2 Dead-Peer-Detection (/Setup/VPN/IKEv2/General/DPD-Inact-Timeout) wird nicht mehr nur ein Intervall von 60 Sekunden ausgeführt.

→ Das Weiterleiten von IPv4-Fragmenten (/setup/ip-router/1-N-NAT/Fragments/) bei gleichzeitiger QoSLimitierung wird nicht mehr als Angriff gewertet. Dadurch ist eine Kommunikation wieder möglich.

→ Ein unvermittelter Neustart des Routers während des Zugriffs auf Zertifikatsinformationen der SCEP-CA wurde behoben.

→ Es wurde ein Fehler behoben, bei dem für WEBconfig ein falsches Zertifikat verwendet wurde.
→ Beim Ändern des Router-Passwortes eines Benutzers mit administrativen Rechten werden nun auch Passwörter mit mehr als 15 Stellen akzeptiert.
→ Der SNMP Port 161 wird in der Konfiguration eines LANCOM Routers nicht mehr als geschlossen angezeigt, obwohl SNMPv3 auf dem WAN erlaubt ist.
→ Die Dienste SNMPv2 und SNMPv3 können separat angezeigt werden.
→ Beim LANCOM-internen SCEP-Client kann ein CA-Fingerprint übernommen werden, auch wenn dieser länger als 59 Zeichen ist.

VPN

→ Eine IKEv2 VPN-Verbindung wird nicht mehr nach einiger Zeit getrennt, wenn die Dead Peer Detection (DPD) aufgrund einer nicht mehr vorhandenen Child-SA keine Verbindung zur VPN-Gegenstelle mehr erkennen kann.
→ Ein auf nur einer Seite eingerichteter L2TP-Tunnel führt nicht mehr dazu, dass ein bereits bestehender aktiver zweiter L2TP-Tunnel zwischen den beiden Routern getrennt wird.
→ Eine innerhalb eines Scripts ausgeführte Konfigurationsänderung mittels Sleep-Befehl führt nicht mehr dazu, dass ein IKEv1-IPSec-Tunnel getrennt und nicht mehr aufgebaut wird.
→ Ein „default -r“ in einem Skript führt nicht mehr dazu, dass ein VPN-Tunnel nicht aufgebaut werden kann.
→ Wenn ein LANCOM Router eine IKEv2-Verbindung auf dem LAN angenommen hat, wird die Verbindung auch dann aufgebaut, wenn die Quell-Adresse das Routing-Tag 0 aufweist.

WLAN

→ Die RADIUS-Authentifizierung (IEEE 802.1x) von WLAN-Clients in einem WLC-Szenario wird nicht mehr mit der Trace-Fehlermeldung „missing private key“ abgebrochen.
→ Die Anmeldung am Public Spot über ein deaktiviertes Benutzerkonto ist über den Assistenten „Public-Spot Benutzer verwalten“ auch dann nicht mehr möglich, wenn der Benutzer in der Auto-ReLogin-Tabelle eingetragen ist.
→ Access Points können sich wieder per Auto-WDS verbinden, auch wenn das zu verwendende Frequenzband im Auto-WDS-Profil fest auf „nur 5GHz“ eingestellt ist.
→ In einem Public-Spot Szenario mit PMS-Anbindung ist der Link zur Anmeldung über einen Voucher auf der Login-Seite wieder vorhanden, auch wenn die Spracheinstellung des WLAN-Clients auf Französisch oder Italienisch eingestellt ist.

→ Ein unvermittelter Neustart des Routers, ausgelöst durch die Verwendung der Public-Spot Benutzertabelle (/setup/public-spot-module/user-table), wurde behoben.
→ Bei erneutem Ausdruck eines Vouchers über den Public-Spot-Benutzerverwaltungs-Assistenten wird das Volumen-Budget auf den integrierten Templates des Gerätes wieder korrekt angezeigt.
→ Die IPv6-Datenkommunikation per WLC-Tunnel zwischen einem WLAN-Client und einem LANCOM WLAN-Controller funktioniert wieder.

VoIP

→ Bei der Übergabe einer DNS-Auflösung an den Voice Call Manager (VCM) kommt es nicht mehr zu einem unvermittelten Neustart des Routers.
→ Ein Konfigurations-Update der DECT-Basisstation LANCOM DECT 510 IP funktioniert auch nach einer Adress-Änderung des Provisioning Update-Servers (/Setup/Provisioning-Server). Die Basisstation wird nun auch nach einer Änderung der Update-URL über die Konfigurationsänderung informiert.
→ Mehrere Handsets an derselben Basisstation können wieder die gleichen SIP-User verwenden.
→ DECT-Basisstationen werden in der Statustabelle nicht mehr mit falscher IP-Adresse hinterlegt. Der dadurch ausgelöste Anzeigefehler im LANmonitor ist behoben.
→ Nach einem Software Reboot (Warmstart) kann auch bei Verwendung einer externen SIP-Trunk-Leitung eine Verbindung zum SIP-Server wieder hergestellt werden. Eine Trennung der Stromzufuhr (Kaltstart) ist nicht mehr notwendig.
→ Bei Verwendung einer SIP-Trunk-Leitung kommt es nicht mehr dazu, dass das „to-Feld“ im SIP-Header nicht korrekt in das E.164-Format überführt wird.
→ Bei zwei konfigurierten SIP-Trunks ist es wieder möglich, einen Ruf von einem der SIP-Trunks zu einem SIP-Einzelaccount durchzustellen.
→ Im All-IP-Assistenten ist der „Registered-Mode“ bei einem Telekom SIP-Trunk nun im Default aktiv.

LCOS Änderungen 9.24.0153 RU3

Wichtiger Hinweis zum Update:
In der Default-Konfiguration ist der SNMP-Zugriff über eine WAN-Schnittstelle deaktiviert. Falls der WANZugriff für SNMP manuell per Konfiguration aktiviert wurde, muss bei Bedarf nach dem Firmware-Update der Zugriff für SNMPv1/SNMPv2 manuell aktiviert werden. Die vorherige Konfigurationseinstellung für SNMP bleibt für SNMPv3 erhalten.

Korrekturen / Anpassungen

Network Connectivity

→ Es wurde ein Fehler behoben, der zu Störungen bei Clearmode-Verbindungen führte.
→ Es wurde ein Fehler behoben, bei dem abgehende Anrufe über eine SIP-Leitung gestört waren.
→ Skripte können wieder über einen WLC ausgerollt werden.
→ Der Re-Keying-Mechanismus bei IKEv2 wurde verbessert.
→ IKEv2-VPN-Verbindungen werden wieder zuverlässig aufgebaut.
→ IP-Telefone können sich über den SIP-ALG wieder an einer übergeordneten VoIP-TK-Anlage anmelden.
→ Wenn mehrere SIP-Trunks oder Einzel-Accounts konfiguriert sind, werden ausgehende Rufe wieder über die vorgesehene Leitung aufgebaut.
→ Unnötige WLAN-Modem-Load-Informationen wurden aus dem Bootlog entfernt.

WLAN

→ Die Bestätigungsseite nach einem erfolgreichen Login an einem Public Spot wird wieder früher ausgeblendet.
→ Es wurde ein Problem behoben, bei dem sich kein Client mehr zu einem WLAN verbinden konnte.
→ Stabilitätsverbesserungen für 802.11ac P2P-Strecken

LCOS Änderungen 9.24.0076 RU2

Wichtiger Hinweis zum Update

In der Default-Konfiguration ist der SNMP-Zugriff über eine WAN-Schnittstelle deaktiviert. Falls der WAN-Zugriff für SNMP manuell per Konfiguration aktiviert wurde, muss bei Bedarf nach dem Firmware-Update der Zugriff für SNMPv1/SNMPv2 manuell aktiviert werden. Die vorherige Konfigurationseinstellung für SNMP bleibt für SNMPv3 erhalten.

Korrekturen / Anpassungen

Network Connectivity

→ Zuverlässige Initialisierung des integrierten VDSL-Modems in bestimmten Situationen.

LCOS Änderungen 9.24.0075 RU1

Wichtiger Hinweis zum Update

In der Default-Konfiguration ist der SNMP-Zugriff über eine WAN-Schnittstelle deaktiviert. Falls der WANZugriff für SNMP manuell per Konfiguration aktiviert wurde, muss bei Bedarf nach dem Firmware-Update der Zugriff für SNMPv1/SNMPv2 manuell aktiviert werden. Die vorherige Konfigurationseinstellung für SNMP bleibt für SNMPv3 erhalten.

Korrekturen / Anpassungen

Network Connectivity

→ Die Zugriffsrechte für SNMPv2 können jetzt separat geschaltet werden.

→ Es wurde ein Problem behoben, welches dazu führte, dass die HTTPs-Kommunikation von einem Apple-Gerät mit iOS 10 oder macOS 10.12 zu einem LANCOM nicht mehr funktionierte.

→ Ein Problem mit der LANCOM DECT 510 IP wurde behoben.

LCOS Änderungen 9.24.0070 Rel

Neue Features

Network Connectivity

→ Unterstützung von Auto-Provisionierung für das LANCOM DECT 510 IP
→ Unterstützung von Call-Forking im Voice Call Manager
→ Unterstützung der SIP-Methoden PRACK und UPDATE
→ Unterstützung von Message Waiting Indication im Voice Call Manager
→ Verfügbare Rx/Tx-Bandbreite kann bei Routern mit integriertem VDSL-/ADSL-Modem manuell konfiguriert werden.

WLAN

→ Im Public Spot gibt es nun vordefinierte Bandbreitenprofile.
→ Unterstützung von RADIUS CoA (Change of Authorization) im Public Spot

LCOS Änderungen 9.20.0683 RU2

Wichtiger Hinweis zum Update:
Vor dem Update der LANCOM 1631E, LANCOM 831A und Business LAN R800A auf LCOS 9.20 muss der Loader 4.18 eingespielt werden.

Korrekturen / Anpassungen

Network Connectivity

→ Es wurde ein Problem mit dem Jitter-Buffer behoben, welches beim Faxversand dazu führte, dass die Faxübertragung abbrach.
→ Ein Zugriff auf eine bestimmte Konfiguration in der WEBconfig verursacht keinen Neustart des Geräts mehr.
→ Um Probleme auf der Serverseite zu vermeiden, liest der HTTP-Client die komplette Serverantwort, wenn eine Anmeldung benötigt wird, bevor eine weitere Anfrage gestartet wird.
→ IKEv2-VPN in Verbindung mit NAT-Traversal funktioniert wieder wie vorgesehen.
→ Es wurde ein Problem mit der Auswahl der Codecs behoben, wenn ein Telefon direkt am LANCOM angeschlossen ist.
→ CLIP no Screening funktioniert wieder wie vorgesehen, wenn eine Telefonanlage über die S0-Schnittstelle mit dem LANCOM verbunden ist.

LCOS Änderungen 9.20.0647 RU1

Wichtiger Hinweis zum Update:
Vor dem Update der LANCOM 1631E, LANCOM 831A und Business LAN R800A auf LCOS 9.20 muss der Loader 4.18 eingespielt werden.

Korrekturen / Anpassungen

Network Connectivity

→ BGP-Pakete werden ab sofort mit DSCP CS6 markiert.
→ Die Routen bei der Einwahl mit vereinfachten Zertifikaten bei IKEv1 werden wieder korrekt gesetzt.
→ Die Tabelle für die automatische VLAN-Providerauswahl ist jetzt editierbar.
→ Die Markierungen von DiffServ-Tags von inneren Tunneln wie PPTP, L2TP, GRE oder EoGRE werden jetzt auf den äußeren VPN-Tunnel übernommen.
→ Verbesserungen beim IKEv2-Rekeying.
→ Verbesserungen bei der Interoperabilität von TLS-1.2-Verbindungen.
→ RIP propagiert eine konditionale Route wieder wenn die Gegenstelle verbunden ist.
→ ICMP-Polling funktioniert wieder gegen Loopback-Adressen
→ Der Zähler für aktive Rufe im Voice-Call-Manager wurde korrigiert.
→ Im LANmonitor wird nun die Firewallregel angezeigt, bei der die erste Aktion greift.
→ Wird auf der LAN-Schnittstelle ein Broadcast empfangen und verworfen, wird dafür keine Syslog-Nachricht mehr verschickt.
→ SMS können wieder über den LANmonitor gesendet und gelöscht werden.
→ Verbesserungen des SIP-ALG im Zusammenspiel mit Mitel Telefonanlagen. OPTIONS-Pakete werden vom richtigen Port versandt.
→ SIP-ALG: Die Behandlung von Multipart Bodies in der SIP-Message wurde hinzugefügt.
→ SIP-ALG: Es wurde ein Problem behoben, bei dem das Routing zwischen lokalen Netzen in Verbindung mit Policy-Based Routing nicht funktionierte.
→ Wird ein Ruf von einem analogen Telefon weitergeleitet, führt dies nicht mehr zu einseitiger Sprachübertragung.
→ Der Rollout-Agent startet nun auch den Rollout, wenn eine Config-Server-URL nicht per DHCP-Option 43 übermittelt wird, aber in der Gerätekonfiguration hinterlegt ist.
→ Probleme im Zusammenspiel mit der Swyx behoben (CTI+, Rufweiterleitung, etc.)
→ Unterstützung von Deutsche Telekom vSDP der SIP-Methoden PRACK und UPDATE nach 1TR114

WLAN

→ Die interne Anordnung der WLAN-Module des OAP-830 wurde getauscht, um die WLAN-Performance zu verbessern. Bitte beachten Sie beim Betrieb von Punkt-zu-Punkt-Strecken mit diesem Gerät folgenden Knowledge-Base-Artikel: http://www2.lancom.de/kb.nsf/0/FB780A27309985EBC1257FF00029F4CF?opendocument

→ Es wurde ein Problem behoben, bei dem entfernte Access Points keine Konfiguration von einem WLC erhalten haben, wenn auf der WAN-Verbindung eine zu große MTU ausgehandelt wurde.

→ Wird bei einer 802.11ac-Verbindung ein Access Point im Client-Modus betrieben, kann sich dieser wieder an einer Basisstation anmelden.

LCOS Änderungen 9.20.0566 Rel

Wichtiger Hinweis zum Update:
Vor dem Update der LANCOM 1631E, LANCOM 831A und Business LAN R800A auf LCOS 9.20 muss der Loader 4.18 eingespielt werden.

Korrekturen / Anpassungen

Network Connectivity

→ Es wurde ein Problem bei der Faxübertragung mittels T.38 behoben.

→ Wird der WEBconfig All-IP Assistent ein weiteres Mal ausgeführt, werden nun alle vorherigen Einstellungen wie vorgesehen ersetzt.

→ PPTP-Tunnel werden wieder aufgebaut, nachdem ein Eintrag in der Backup-Tabelle hinzugefügt wurde.

→ Ein Problem mit erzwungener Bandbreitenreservierung wurde behoben.

WLAN

→ Clients mit einem Intel AC-7260 Chipsatz können sich wieder mit einem Access Point verbinden, wenn dieser im „ac only“ Modus arbeitet.

→ Eine Anmeldung über 802.1x funktioniert wieder unter hoher Paketlast bei APs mit 11ac.

→ CAPWAP setzt keine Host-Routen mehr auf Ziele im lokalen Netz, wenn via WLC eine statische IP vergeben wurde.

LCOS Änderungen 9.20.0517 RC2

Wichtiger Hinweis zum Update:
Vor dem Update der LANCOM 1631E, LANCOM 831A und Business LAN R800A auf LCOS 9.20 muss der Loader 4.18 eingespielt werden.

Korrekturen / Anpassungen

Network Connectivity

→ Ein Fehler im All-IP Assistenten wurde behoben, bei dem nicht alle Einträge wie vorgesehen gelöscht wurden.
→ Wird eine L2TP-Gegenstelle getrennt, werden entsprechende gelernte RIP-Routen nicht mehr weiter verteilt.
→ Nach Rückfall auf 2G verbleibt der Router nicht mehr dauerhaft im Edge-Modus.
→ Der iPerf-Server-Daemon ist wieder über VPN erreichbar, wenn der Zugriff über WAN auf VPN eingeschränkt ist.
→ Es wurde ein Problem behoben, bei dem sich eine SIP-Leitung aufgrund fehlender DNS-Auflösung nicht mehr registrieren konnte.
→ SIP-Pakete mit einem Inhalt >1024 Byte werden nicht mehr abgeschnitten.
→ Der iPerf-Server-Report wird wieder vom iPerf-Client empfangen, wenn die Client-Pakete einen VLAN Tag enthalten.
→ Wird ein Gespräch auf Halten gelegt, wird eine eventuelle Wartemusik wieder korrekt abgespielt.

WLAN

→ Location Based Services (LBS) ist nicht mehr auf Geräten ohne WLAN oder WLC Option konfigurierbar.
→ Die Public Spot Template Vorschau ist nur noch sichtbar, wenn eine Public Spot Option auf dem LANCOM vorhanden ist.
→ Ein konfigurierter Public Spot Login Text wird wieder korrekt angezeigt.
→ Verringerter Speicherverbrauch bei aktivierter Aggregierung und 802.11n Karten.

LCOS Änderungen 9.20.0385 RC1

Wichtiger Hinweis zum Update:
Vor dem Update der LANCOM 1631E, LANCOM 831A und Business LAN R800A auf LCOS 9.20 muss der Loader 4.18 eingespielt werden.

Neue Features

Network Connectivity

→ Unterstützung eines automatisierten Rollouts mittels DHCP-Option 43
→ Der SCEP-Client beachtet nun Abhängigkeiten zwischen Zertifikaten.
→ Unterstützung von DTMF Umwandlung für All-IP
→ Unterstützung von SNMPv3
→ Der Voice-Call-Manager unterstützt nun TCP für SIP-Verbindungen.
→ Unterstützung von Voice over Secure IP (SIPS/SRTP) im Voice-Call-Manager
→ Bei ll2mdetect wird nun die Anzahl der gefundenen Geräte angezeigt.
→ Im ADSL/VDSL Status wird nun angezeigt wie lange das Modem synchron ist und wie viele Verbindungen es gab.
→ Der NTP-Client und Server unterstützen nun IPv6.
→ Es können nun EAP-TLS Einstellungen vorgenommen werden, wenn der LANCOM als 802.1x Supplicant agiert.
→ Unterstützung von IKEv2
→ Unterstützung von BGPv4
→ Im Status wird nun angezeigt, ob eine Backup-Verbindung aktiv ist und wie oft eine Backup- Verbindung aufgebaut wurde.
→ Es kann nun ein Backup ausgelöst werden, wenn eine gelernte Route nicht mehr verfügbar ist (Route Monitor).
→ Die IPv6-Firewallregel „Allow-IPSec“ ist nun im Default aktiv.
→ DNS-Anfragen können nun per Syslog an einen externen Syslog-Server weitergeleitet werden.
→ LCOScap unterstützt nun IPv6
→ Unterstützung von IPv6 VPN mit IKEv1/IKEv2
→ Der Syslog-Server kann nun auch als DNS-Name oder IPv6-Adresse eingetragen werden.
→ SIP-Nachrichten werden auf Wunsch nur vom SIP-Registrar akzeptiert.
→ Unterstützung von Overlap Dialing für SIP-Trunks
→ Prio Tags werden auf WAN-Verbindungen in den VLAN-Header gemäß 1TR-112 oder nach DSCP übernommen
→ Erweiterte Unterstützung von TR.069 und TR.181

→ Lehnt der RADIUS-Server eine Authentifizierungsanfrage ab, wird im Syslog der Grund für die Ablehnung ausgegeben.
→ Unterstützung von ChaCha20-Poly1305 für SSH
→ Die CA unterstützt nun die SCEP-Nachricht GetCaCaps.
→ Die Default Gruppen für IKE und PFS im VPN wurden auf DH-Gruppe 14 angepasst.
→ Bei Konfigurationsänderungen werden registrierte SIP-User nicht entfernt.
→ Unterstützung von Parallelruf im ISDN
→ Unterstützung von IPerf als Server und Client
→ Konfigurationsprotokolle sind jetzt schaltbar.
→ In WEBconfig werden nun unter dem Reiter „Dienste“ die offenen Ports angezeigt.
→ Das Powersaving der Ethernet-Schnittstellen ist nun im Default deaktiviert.
→ Der VLAN-Tagging-Modus „Ankommend gemischt“ wurde entfernt.
→ Die DHCP-Leasedauer ist nun pro Netzwerk konfigurierbar.
→ Passwortkomplexität für das Hauptgerätepasswort und weitere Administratoren kann erzwungen werden.

WLAN

→ Bei bestehendem CAPWAP-Tunnel wird IAPP deaktiviert.
→ Unterstützung von Airtime Fairness
→ Die Funkfeldoptimierung kann nun auch auf unabhängigen Access Points durchgeführt werden.
→ Auf einem WLC sind nun mehrere AutoWDS-Profile konfigurierbar.
→ Unterstützung von Adaptive RF Optimization
→ Unterstützung von Wireless Intrusion Detection System (WIDS)
→ Auf einem WLC können nun die durchschnittlichen WLAN-Fehlerraten der einzelnen Access-Points ausgelesen werden.
→ Mit der URL-Variable „%r“ kann nun in einem Public Spot Redirect die MAC des Access-Points übermittelt werden, an dem sich der Client angemeldet hat.
→ Die absolute Ablaufzeit eines Public Spot Vouchers kann nun auch in Minuten und Stunden konfiguriert werden.
→ Es gibt nun einen Zähler der die fehlgeschlagenen WPA-Anmeldeversuche anzeigt.
→ Die vorgegebenen Datenraten können nun pro SSID konfiguriert werden.
→ Die Public Spot Funktion „AGBs akzeptieren“ ist nun auch bei Verwendung von PMS nutzbar.
→ Für den Public Spot Manage-User-Assistenten kann festgelegt werden, welche Spalten angezeigt werden sollen.

→ Überflüssige Leerzeichen bei der Eingabe von Benutzernamen und Passwörtern im Public Spot werden automatisch entfernt.
→ Das dem Public Spot User zugewiesene Bandbreitenprofil kann nun auf dem Voucher ausgeben werden.
→ Zum Schutz vor Brute-Force Angriffen im Public Spot ist nun eine Login-Sperre konfigurierbar.
→ Es ist nun schaltbar, ob HTTPS-Verbindungen von nicht angemeldeten Clients an das Public Spot Gateway weitergeleitet werden sollen.
→ Über die WEBconfig gibt es nun eine Vorschaumöglichkeit der hochgeladenen Public Spot Templates.
→ Unterstützung von Spectral-Scan für 802.11ac WLAN-Module.
→ Die WLAN-Ratenadaption wurde verbessert.
→ Die aktuelle Kanalbreite sowie das aktuell benutzte MCS werden nun in der WLAN-Interpoints-Tabelle und der Stations-Tabelle angezeigt.

Korrekturen / Anpassungen

Network Connectivity

→ Es wurde ein Fehler behoben, der zu einem Neustart des Routers führte wenn der SMS-Eingang über WEBconfig aufgerufen wurde.
→ Es wurde ein Problem mit der DNS-Auflösung behoben, bei dem eine explizite DNS-Weiterleitung konfiguriert werden musste.
→ Eine Portweiterleitung der VPN-Ports 500 und 4500 funktioniert wieder.
→ Die Firewall-Paketaktion „Nur wenn Default-Route“ wird wieder korrekt behandelt.
→ Die Variable „DEVICE_URL“ funktioniert im Befehl „loadscript“ wieder korrekt.
→ Wird ein VPN-Tunnel über DynDNS Namen aufgebaut, so wird nun nach einer Trennung der Name sofort erneut aufgelöst und der Tunnel nicht an die alte Adresse aufgebaut.
→ Ein Ruf eines SIP-Telefons über den SIP-ALG, welches PRACK nutzt, wird nicht mehr getrennt.
→ Der Assistent „Internet-Zugang einrichten“ über die WEBconfig, setzt die Netzmaske wieder korrekt.
→ Es wurde ein Problem behoben, welches zu einem Neustart des LANCOM aufgrund von Speichermangel führte.
→ Eine Dynamic VPN-Verbindung kann über einen Load-Balancer wieder aufgebaut werden.
→ Die Zeitangabe in der IPerf-Statustabelle wird nun deutlicher dargestellt.
→ Ausgehende SIP-Trunk-Leitungen einer Telefonanlage über den SIP-ALG werden nicht mehr getrennt.

→ Die ausgehandelte MTU einer WAN-Schnittstelle für IPv6 wurde korrigiert.
→ Es wurde ein Fehler behoben, bei dem eine 4G-Backup-Verbindung nicht aufgebaut werden konnte.

WLAN

→ Es wurde ein Problem behoben, bei dem sich nur bestimmte Clients an einem 802.11ac Access Point anmelden konnten.
→ Ein Fehler führte dazu, dass ein Access Point im Client-Modus beim Roaming zwischen denBasisstationen mehrere Minuten nicht mehr erreichbar war.
→ Bei Geräten mit wenig freiem Speicher kann die Konfiguration wieder geschrieben werden.
→ Die Prüfung der Antwort des DNS-Servers erfolgt nun case-insensitive.
→ Ein Zertifikatsfehler wurde behoben, bei dem ein Access Point versucht sich mit einem WLC zu verbinden.

5. 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.