LANCOM Release Notes

LCOS

10.30 Rel

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

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

09.05.2019, 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 10.30 Rel 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 10.30

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 10.30 entfällt die Unterstützung für folgende Geräte

- LANCOM 831A
- LANCOM IAP-322
- LANCOM L-451agn
- LANCOM L-452agn
- LANCOM L-460agn
- LANCOM OAP-3G

Für die LANCOM Access Points der E-Serie folgt die Unterstützung der LCOS 10.30 zu einem späteren Zeitpunkt.

3. Hinweise zu LCOS 10.30

3.1 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 10.30

4.1 Feature-Highlights

SD-WAN – Application Routing

Profitieren Sie von einem deutlichen Performance-Gewinn bei der Nutzung moderner Cloud-Anwendungen (z.B. Office 365, SalesForce, etc.). SD-WAN Application Routing kann Cloud-basierte Anwendungen erkennen und leitet diese direkt ins Internet (Local Break-out). Dies entlastet die VPN-Strecke zur Zentrale als auch die Internetleitung in der Zentrale.

SD-WAN – Layer-7-Applikationskontrolle in der Firewall

Bewahren Sie die Kontrolle über die Nutzung der Anwendungen in Ihrem Netzwerk. Durch die Definition anwendungsbezogener Regeln in der Firewall liegt es in Ihrer Entscheidung, welche Internet-Anwendungen erlaubt, gesperrt, limitiert oder priorisiert werden.

WLC-Funktionen im vRouter (vWLC)

Entscheiden Sie selbst und flexibel, welche Rolle Ihr LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC). Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl verwalteter Access Points ist abhängig von der Lizenzkategorie des vRouters.

4.2 Weitere Features

TLS 1.3

Die Unterstützung des neuen Protokolls TLS 1.3 erhöht die Sicherheit beim Gerätezugriff über WEBconfig.

IKEv2 Elliptic Curve Digital Signature Algorithm (ECDSA)

IKEv2 unterstützt ab sofort die Authentifizierungsmethode Elliptic Curve Digital Signature Algorithm (ECDSA). Dies ermöglich deutlich kleinere Schlüssellängen und somit höhere Verschlüsselungs-Effizienz bei gleichem Sicherheitsniveau.

IKEv2 Split-DNS

Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen über einen VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird.

IKEv2 Fragmentierung

Ermöglicht die effiziente Fragmentierung von IKEv2-Nachrichten (nach RFC 7383) vom VPN-Router selbst, so dass IKE-Pakete vom Transportnetz nicht mehr fragmentiert werden müssen.

Erweiterung bei Client-Reservierungen im DHCPv6-Server

Im DHCPv6-Server können ab sofort Client-Adressen bzw. Präfixe wahlweise anhand von DUID, MAC-Adresse, Interface-ID (nach RFC 3315) oder Remote-ID (nach RFC 4649) zugewiesen werden.

Doppelte Anzahl an Public Spot-Usern

Für die LANCOM 178x- und 179x-Serie mit Public Spot Option erhöht sich die Anzahl der User von 64 auf 128.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 5 „Historie LCOS 10.30“.

5. Historie LCOS 10.30

LCOS-Änderungen 10.30.0075 Rel

Korrekturen / Anpassungen

Allgemein

- Bezog ein Router oder Access Point seine IP-Adresse per DHCP, kam es beim Empfang von IP-Paketen außerhalb des lokalen Netzwerkes auf dem DHCP-Interface zu einem Fehler beim Auflösen der Routen. In der Folge lehnte die Firewall des Gerätes die IP-Pakete mit der Meldung „Intruder detection“ ab.
- 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.
- Wenn ein LANCOM Router die IP-Parameter für die Gegenstelle INTERNET-DEFAULT von einem DHCP-Server bezog und ein vorgeschaltetes Gateway die IP-Adresse xx.xx.xx.254 besaß, kam es zu einem IP-Adresskonflikt, da der LANCOM Router sich selbst ebenfalls die IP-Adresse xx.xx.xx.254 vergab. Dies führte dazu, dass keine Kommunikation zum Internet und somit auch nicht zur LMC möglich war.
- Das Ausrollen einer Konfiguration von der LANCOM Management Cloud (LMC) an einen Router, welcher über einen IPv6 Dual Stack-Lite-Anschluss mit dem Internet verbunden war, konnte zu einem unvermittelten Neustart des Routers führen.
- Wurde ein DS-Lite-Tunnel in einem Load-Balancer hinterlegt (IP-Router / Routing / Load-Balancing), konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.
  Der DS-Lite-Tunnel kann jetzt im Load-Balancer nicht mehr ausgewählt werden.
- Wurde IKEv2 in Verbindung mit IPv6 im LAN verwendet, konnte der IKE-Config-Mode-Server einem VPN-Client keine IPv6-Default-Route zuweisen.
- Bezog ein LANCOM Router seine IP-Parameter für ein mit einem Schnittstellen-Tag versehenes Netzwerk per DHCP, wurde die automatisch generierte Default-Route Netzwerken mit anderen Schnittstellen-Tags zugewiesen.
- Dies führte dazu, dass Pakete aus den betroffenen Netzwerken falsch geroutet wurden, anstatt die Pakete zu verwerfen.
- Nach Ausführen des Befehls default -r auf der Root-Ebene zwecks Zurücksetzen der Konfiguration auf die Standard-Werte wurde die Tabelle „Setup/Firewall/DNS-Destinations“ nicht zurückgesetzt.
- Beim LANCOM vRouter fehlte die Funktion zur Ermittlung und Festlegung von Daten- und Zeit-Budgets.
- Bei den LANCOM Geräten ISG-4000 und WLC-1000 war es nicht möglich, eine alternative Boot-Konfiguration zu erstellen.
- Bei Webseiten-URLs, welche in der Konfiguration des Content Filters als Whitelist-Einträge angelegt waren, dauerte der Aufbau der Webseiten-Inhalte ungewöhnlich lange.
- Die Checksummen-Berechnung von Ethernet-Paketen funktionierte im vRouter nicht korrekt. Dies konnte zu Kommunikationsproblemen führen.

VPN

- Nahm ein Router eine VPN-Verbindung an, bei welcher die Authentifizierung per RADIUS-Server erfolgte, blieben die VPN-Regeln der Verbindung auch nach Deaktivierung des VPN-Moduls und Abbau der Verbindung in der SADB aktiv. Es wurden weiterhin DPD-Pakete versendet.
- Split-DNS soll DNS-Informationen über den IKE-Config-Mode übertragen. Hierbei wurden Domänen, die im DNS-Server als Subdomain hinterlegt wurden, nicht übertragen, sondern nur die, welche als eigene Domäne für den Router konfiguriert waren. Zusätzlich führte eine leerer Eintrag bei der Geräte-eigenen Domäne zu einem Anzeigefehler in der entsprechenden Status-Tabelle des empfangenden Gerätes.
- Bei der Verwendung der Split-DNS-Funktion in einer IKEv2-VPN-Verbindung wurde beim Übermitteln des DNS-Wildcard-Wertes „*“ im Client-Router der Wildcard-Wert „*.“ eingetragen. Somit wurde der Wildcard-Eintrag in der Außenstelle nicht korrekt verwendet.
- Bei Verwendung von IKEv2-Verbindungen besteht die Möglichkeit, die Authentifizierung über einen externen RADIUS-Server durchzuführen. Dabei wurden RADIUS-Anfragen vom LANCOM Router nicht wieder freigegeben, sodass nach längerem Betrieb keine weiteren RADIUS-Anfragen zur Authentifizierung mehr gestellt werden konnten. In der Folge konnten keine VPN-Verbindungen mehr aufgebaut werden.
- War für eine IKEv2-Verbindung ein Eintrag in der Polling-Tabelle hinterlegt und der IKE-Config Mode „Client“ definiert, damit die Pakete hinter der zugewiesenen IP-Adresse maskiert werden, so funktionierte der VPN-Verbindungsaufbau nicht.
- Wenn eine VPN-Gegenstelle (IKEv1), welche über eine IPv6-WAN-Verbindung aufgebaut werden sollte, und eine ISDN-Gegenstelle die gleiche Namensbezeichnung hatten, konnte die VPN-Gegenstelle nicht korrekt aufgebaut werden.
- Bei der Verwendung von GCM-Verschlüsselungs-Algorithmen trennte eine fehlerhafte VPN-Verbindung, die über einen externen RADIUS-Server authentifiziert werden sollte, alle aufgebauten VPN-Verbindungen, welche erfolgreich über den RADIUS-Server authentifiziert wurden.
- Wenn in einem Einwahl-Profil des LANCOM Advanced VPN Client im Menü „Erweiterte IPsec-Optionen / UDP-Encapsulation“ der Port 4500 fest eingestellt wurde, scheiterte eine IKEv1-Client-Einwahl mit der Fehlermeldung „IKE info: Phase-2 proposal failed“.
- Wenn eine VPN-Verbindung (manuell) getrennt und dann neu verbunden wurde (Reconnect), funktionierte das OSPF-Protokoll über diese VPN-Verbindung nicht mehr.

WLAN

- Wenn auf einem LANCOM Gerät sowohl ein WLAN als auch die Public Spot-Funktion betrieben wurde, hatte dies zur Folge, dass Public Spot-Benutzer nach Erreichen des standardmäßig definierten WLAN-Idle-Timeout nicht nur aus der WLAN-Stations-Tabelle, sondern auch aus der Public Spot-Auto-Relogin-Tabelle gelöscht wurden. Ein erneutes Anmelden am Public Spot mit den gleichen Benutzerdaten war somit nicht mehr möglich.

VoIP

- Empfing ein LANCOM Router ein codiertes T.38-Paket ohne Audio-Inhalte, so konnte dies zu einem unvermittelten Neustart des Routers führen.
- Sendete eine SIP-TK-Anlage ein INVITE mit einem sehr kleinen Session Timer, wurde dieser vom LANCOM Router übernommen. Wurde dieser Wert vom Provider mit der Meldung „422 Session Interval Too Small" quittiert (mit Angabe des minimalen Session Timers), ignorierte der Router dies, wenn der Provider während der „Early Media Phase" ein UPDATE sendete. In der Folge baute der Router das Gespräch nach Ablauf des ursprünglichen Session Timers mit einem BYE ab.
- In einem Szenario mit einem Telekom SIP-Trunk bzw. Telekom All-IP-Anschluss und einer per SIP-Trunk angebundenen NFON Cloud-TK-Anlage wurde ein eingehender Anruf über den Telekom-Anschluss von NFON mit der Meldung „404 Not Found" abgelehnt.
  Die Ursache dafür war, dass NFON bei Verwendung eines SIP-Trunks die User-ID im Feld P-Asserted-Identity anstatt in der P-Preferred-Identity erwartet.
- Bei der Verwendung von ISDN-Endgeräten, welche bei einem ausgehenden Anruf keine Quellrufnummer sendeten (z.B. eine Türsprechanlage) konnten ausgehende Gespräche nicht geführt werden, wenn ein ein VoIP-Provider verwendet wurde, welcher das leere oder mit dem Wert „anonym" gefüllte „Calling Party"-Feld nicht akzeptierte (z.B. SIPGATE).
- Bei einem eingehenden Telefonat über eine SIP-PBX-Leitung wurden DTMF-Signale nicht an die Teilnehmer weitergeleitet.
- Wurde vom SIP-Provider aufgrund einer aktiven Rufweiterleitung die Meldung „181 Call Is Being Forwarded" auf einen ausgehenden Anruf empfangen, fehlten in der vom Provider geforderten Bestätigung (mittels PRACK) Informationen im To-Header. Dadurch baute der Provider den Anruf mit der Meldung „481 Call/Transaction Does Not Exist" ab.
- Es konnte zu Gesprächsabbrüchen nach ca. 15 Minuten kommen, da der Voice-Call-Manager auf eine UPDATE-Anfrage des VoIP-Providers nach 15 Minuten mit der Meldung "200 OK" antwortete und in dieser Antwort SDP-Informationen enthalten waren, welche der VoIP-Provider nicht verarbeiten konnte.
  In der Folge sendete der VoIP-Provider eine BYE-Nachricht, was dazu führte, dass das Telefonat beendet wurde.
- Sendete ein SIP-Teilnehmer ein REGISTER-Paket ohne Angabe des Ports im Contact-Header, hängte der Voice Call Manager im darauf folgenden 200 OK im Contact-Header den Port 0 an. In der Folge konnte es zu fehlender Sprachübertragung bei eingehenden Anrufen kommen.
- Bei eingehenden Anrufen konnte es bei der Umwandlung eines DTMF-Signals zu einem Fehler kommen, in Folge dessen alle RTP-Pakete verworfen und eingehende Sprachdaten nicht übertragen wurden.

LCOS-Änderungen 10.30.0045 RC2

Neue Features

Allgemein

- Für das CLI-Kommando „ll2mdetect“ kann nun ein Ziel-Interface angegeben werden (Parameter „-i“).
- Das CLI-Kommando „show job“ gibt nun zusätzlich die gesamte CPU-Last aus.

Korrekturen / Anpassungen

Allgemein

- Nach einem Geräteneustart wurde die in der IPv4-Routingtabelle konfigurierte Distanz nicht mehr beachtet.

WLAN

- Bei Verwendung von WLAN-Routern oder Access Points, die ein 802.11n-WLAN-Modul verwenden, kam es zu Verbindungsabbrüchen mit Amazon Echo-Geräten.
- Der WLAN-Client-Modus unter Verwendung des WLAN-2-Funkmoduls bei den Access Points der LN-17xx-Serie funktionierte nicht.

VoIP

- Bei der Verarbeitung von eingehenden DTMF-Signalen konnte es zum Abbruch der Sprachübertragung kommen.

LCOS-Änderungen 10.30.0028 RC1

Neue Features

Allgemein

- Anpassung der Anzahl gleichzeitiger Public Spot-Benutzer auf Routern der 178x- und 179x-Serie auf 128.
- Die SSL/TLS-Version, die vom internen SMTP-Client verwendet wird, kann nun konfiguriert werden.
- Jitter-Anzeige im ICMP-SLA-Monitor
- „clear"-Kommando zum Leeren der aktuellen Konsolenausgabe
- Unterstützung von TLS 1.3 für WEBconfig
- Unterstützung des ThinAP 2.0-Protokolls zur Anbindung von Wireless ePaper Access Points an einen zentralen Wireless ePaper Server
- Unterstützung von IPv6 für TACACS+
- Unterstützung für RSA-PSS-Signierung in der SCEP-CA

Routing

- Application Routing und -Kontrolle in der IPv4- und IPv6-Firewall
- Auswertung von DSCP-Markierungen in der IPv6-Firewall
- IKEv2-IPv6-CFG-Mode-Adressen können an Clients basierend auf dem vom Provider zugewiesenen Präfix vergeben werden.
- Unterstützung von Adressreservierungen im DHCPv6-Server

VPN

- Unterstützung für IKEv2-Cookie-Notification
- Unterstützung für IKEv2-Split-DNS
- Unterstützung für IKEv2-Fragmentierung
- Unterstützung von ECDSA für die IKEv2-Authentisierung

WLAN

- Die E-Mail-Benachrichtigung für WLAN-Ereignisse kann nun über einen Schalter aktiviert und deaktiviert werden.
- Die Ratenadaption für 802.11n-WLAN-Module berücksichtigt nun bei der Ratenauswahl auch eine konfigurierte Sendeleistungsreduktion.
- Alternativ zur Sendeleistungsreduktion ist nun die Ziel-EIRP (Sendeleistung) im WLAN einstellbar.
- Unterstützung von 802.11k im WLAN-Client-Modus
- Unterstützung von 802.11v im WLAN-Client-Modus
- Unterstützung des Authentisierungsverfahrens SAE im WLAN-Client-Modus

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.