LANCOM Release Notes
LCOS 10.20 RC1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

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

20.06.2018, CBuersch

Inhaltsübersicht

1. Einleitung **2**
2. Neue Features, Änderungen und Historie **2**
LCOS-Änderungen 10.12.0378 RU7 > 10.20.0097 RC1 3
LCOS-Änderungen 10.12.0292 RU6 > 10.12.0378 RU7 6
LCOS-Änderungen 10.12.0243 RU5 > 10.12.0292 RU6 8
LCOS-Änderungen 10.12.0242 RU4 > 10.12.0243 RU5 10
LCOS-Änderungen 10.12.0147 SU3 > 10.12.0242 RU4 11
LCOS-Änderungen 10.12.0146 RU2 > 10.12.0147 SU3 14
LCOS-Änderungen 10.12.0084 SU1 > 10.12.0146 RU2 15
LCOS-Änderungen 10.12.0082 Rel > 10.12.0084 SU1 17
LCOS-Änderungen 10.12.0059 RC2 > 10.12.0082 Rel 19
LCOS-Änderungen 10.12.0041 RC1 > 10.12.0059 RC2 21
LCOS 10.12.0041 RC1 24
3. Wichtige Hinweise **29**
Haftungsausschluss 29
Allgemeine Hinweise 29
Sichern der aktuellen Konfiguration 29
Gerätespezifische Empfehlungen 29
Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes 30

LANCOM Systems

1. Einleitung

LCOS („LANCOM Operating System") ist das Betriebssystem für alle LANCOM Router und Wireless LAN Access Points. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.20 RC1 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 3 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. Neue Features, Änderungen und Historie

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.

LCOS-Änderungen 10.12.0378 RU7 > 10.20.0097 RC1

Mit LCOS 10.20 entfällt die Unterstützung für folgende Geräte

- LANCOM IAP-321
- LANCOM IAP-321-3G
- LANCOM OAP-321
- LANCOM OAP-321-3G
- LANCOM OAP-322
- LANCOM IAP-3G
- LANCOM 1781A-3G

Neue Features

Allgemein

- LANCOM vRouter: Unterstützung von Microsoft Hyper-V
- LANCOM vRouter: Unterstützung von Firmware-Updates via UPX-Dateien
- WEBconfig: Aufrufe der unverschlüsselten Seite auf Port 80 werden automatisch auf die verschlüsselte Seite (Port 443) umgeleitet. Dieses Verhalten ist nach einem Geräte-Reset automatisch aktiv.
- „Boot-Cause“ ist als Umgebungsvariable verfügbar.
- Der RADIUS-Server unterstützt benutzerdefinierte RADIUS-Attribute pro RADIUS-Benutzer.
- Die Suche auf der CLI ist per „find“-Kommando möglich.
- Administratoren aus der Tabelle „Weitere Administratoren“ haben keine Lese- und Schreibrechte mehr in dieser Tabelle.
- Die Readscript-Option „-o“ verhindert die Ausgabe von Passwörtern in Skripten.
- Die DSCP-Markierung für interne Dienste kann nun konfiguriert werden.
- In der Ifx-Tabelle und If-Tabelle der SNMP-IF-MIB sind nun die physikalischen Ethernet-Ports enthalten.

Router & VPN

- Die Konfigurationslogik der IPv6-WAN-Interfaces wurde geändert
- WAN Policy-Based NAT: WAN Policy-Based NAT ermöglicht die Adressumsetzung (Maskierung) von Verbindungen basierend auf Firewall-Regeln.
- DSL-Bridge-Mode für alle LANCOM VDSL-Router: Ab sofort können alle VDSL-Router in einen DSL-Bridge-Modus versetzt werden.
- OCSP-Responder/Server zur Online-Zertifikatsüberprüfung
- Unterstützung für LISP (Locator/ID Separation Protocol)
- Konfigurierbarer VPN-Ziel-Port bei IKEv2 und schaltbare Encapsulation (UDP, HTTPS)
- Anpassung der IKEv1/IPsec-Default-Kryptoalgorithmen/Proposals an aktuelle Standards
- Anpassung der TLS-Default-Kryptoalgorithmen an aktuelle Standards
- Anpassung der SCEP-Default-Kryptoalgorithmen an aktuelle Standards
- BGP: Unterstützung von Redistribution von LISP-Routen
- BGP: Die Administrative Routing-Distanz kann per Policy konfiguriert werden.

- Für das DNS-Forwarding kann eine definierte Absendeadresse konfiguriert werden.
- Neben dem Rollout-Wizard können nun vier weitere programmierbare WEBconfig-Wizards hochgeladen werden.
- Das Formular zur Dynamic VPN-Registrierung ist entfallen.
- Erweiterte Unterstützung der DHCP-Option 43 im DHCPv4-Server
- Unterstützung der DHCP-Option 82 im DHCPv4-Server
- Für den DHCP-Relay-Agent kann eine Absende-Adresse (Loopback-Adresse) konfiguriert werden.
- Die Funktion Automatische WAN-Tag-Erzeugung ist entfallen, siehe hierzu KB-Artikel Einstellungsmöglichkeit zur automatischen WAN-Tag-Erzeugung entfällt.
- Der Schalter zur Konfiguration des Aufbaus der IPSec-SAs wurde entfernt. IPSec-SAs werden nun immer gemeinsam aufgebaut.

WLAN

- **WLAN Client Management**

  Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.
- **LEPS-U**

  Mit LEPS-U (LANCOM Enhanced Passphrase Security - User) vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort für eine SSID.
- Public Spot-Benutzerkonten bzw. RADIUS-Benutzerkonten können per CSV-Datei importiert und exportiert werden.
- Public Spot mit Login nach Einverständniserklärung: Der Zeitpunkt zum Reset der Tages-Account-Limits ist ab sofort konfigurierbar.
- Aktive Public Spot-Sessions werden beim Entfernen des Benutzers über den Manage-User-Wizard beendet.
- Die alte Public Spot-Benutzerliste wurde entfernt und wird nicht mehr unterstützt. Vorhandene Konfigurationen werden automatisch in RADIUS-Einträge konvertiert.
- Unterstützung einer dynamischen Aushandlung der PoE-Leistung durch LLDP anstatt klassenbasiert
- Unterstützung von DSLoL over WLAN auf allen Access Points und WLAN-Routern
- Der Konfigurationspunkt „Nur Unicasts übertragen, Broad- und Multicast unterdrücken“ ist nun für WLCs verfügbar.
- Die WLC-gesteuerte automatische Funkfeldoptimierung berücksichtigt nun auch DFS-Kanäle.

Korrekturen / Anpassungen

Allgemein

- Im LCOS-Pfad ‚/Setup/Certificates/SCEP-CA/Client-Certificates' waren die Felder „Challenge-Passwords" und „General-challenge-password" nicht als Passwort-Felder definiert.

VPN

- Bei der Angabe eines IKEv2-Remote-Gateways konnten maximal 40 Zeichen verwendet werden. Nun können maximal 64 Zeichen eingegeben werden.
- Bekannte Einschränkungen
- Der DHCP-Adressbezug über WLC- oder EoGRE-Tunnel kann aufgrund von Verarbeitungsproblemen bei IP-Paketen fehlschlagen. In seltenen Fällen kann es auch zu einem unvermittelten Neustart des Gerätes kommen.

LCOS-Änderungen 10.12.0292 RU6 > 10.12.0378 RU7

Neue Features

- Unterstützung der Mediasec-Header für verschlüsselte VoIP-Verbindungen
- IKE-Pakete werden nun zur Priorisierung mit DSCP CS6 markiert.

Korrekturen / Anpassungen

Allgemein

- Wurde auf dem Slave-Router VLAN und VRRP gleichzeitig konfiguriert (über LANconfig) oder die Konfiguration importiert (aus einer regulären Konfigurations-Datei oder einer Skript-Datei), so sah dieser die VRRP-Pakete des VRRP-Masters nicht. In der Folge propagierte der Slave-Router sich als VRRP-Master.
- Wenn in der Konfiguration eines LANCOM Mobilfunkrouters ein langer Name für das Mobilfunknetz angegeben war, konnte es bei einem Firmware-Update zu einem unvermittelten Neustart des Gerätes mit anschließendem Rückfall auf die ursprüngliche Firmware-Version kommen.
- Unter der Firmware LCOS 10.12 RU6 eingerichtete Mindestbandbreiten griffen nicht, sofern nur eine Internet-Gegenstelle vom Typ „PPP over Ethernet (PPPoE)“ bzw. „IP over Ethernet (IPoE/DHCPoE)“ auf dem Gerät konfiguriert war.
- Cloud-Ready-Geräte koppeln sich autonom über einen PSK mit der LANCOM Management Cloud. Wurde dieser Vorgang vom Pairing Service einmal abgelehnt, versuchte das Gerät sich weiterhin mit dem PSK zu koppeln, auch wenn der Benutzer das Gerät per Aktivierungscode manuell koppeln wollte.
- In der LLDP-Standard-MIB wurde eine zusätzliche „5“ vor der IP-Adresse angefügt. Dies konnte zu Problemen führen, wenn Monitoring-Programme die IP-Adresse eines Gerätes auslesen wollten.
- Wenn bei einem Gerät der LANCOM 190x-Serie beide VDSL-Modems verwendet wurden, konnte es beim Verbindungsauf- und -abbau zu einer auf der VDSL1-Schnittstelle konfigurierten Internet-Gegenstelle zu einer Fehlermeldung auf der VDSL2-Schnittstelle kommen.

VPN

- Bei zertifikatsbasierten VPN-Verbindungen konnte es zu einem unvermittelten Neustart des Gerätes kommen, wenn das Gerät versuchte, die VPN-Verbindung aufzubauen, während das Zertifikat noch nicht vorhanden war, weil es noch im SCEP-Client errechnet wurde.
- Es konnte sporadisch zu einem unvermittelten Neustart des Gerätes kommen, wenn auf dem Gerät der VPN-Loadbalancer aktiv war und ein Skript, in dem VPN-Parameter definiert waren, eingespielt wurde.
- Wenn bei einer zertifikatsbasierten IKEv2-Verbindung in der Konfiguration ein falscher Zertifikatscontainer referenziert wurde, konnte es zu einem unvermittelten Neustart des Gerätes kommen.

WLAN

- Wenn bei einer iperf Bandbreiten-Messung die IP-Adresse falsch geschrieben wurde (z.B. „iperf c 192.168.5022"), konnte dies zu einem unvermittelten Neustart des Gerätes führen.
- In einem Public Spot Szenario, welches Anmeldungen über ein VLAN getrenntes LAN-Interface annimmt, konnte es vorkommen, dass Benutzer, die zuerst im Public Spot angemeldet waren und danach das VLAN gewechselt haben, nicht mehr mit dem Netzwerk kommunizieren konnten.
- Bei der Verwendung von DSLoL als Gegenstellen-Typ konnte es unter LCOS 10.12 RU6 vorkommen, dass diese Gegenstelle nicht mehr funktionierte.
- Beim LANCOM 1783VAW wurde ein Spectral Scan nicht wie üblich in einem neuen Fenster geöffnet, sondern im gleichen Fenster. Klickte man in diesem Fenster auf die Schalfläche „Zurück", wurde der Spectral Scan jedoch nicht beendet. Erst ein Neustart des Routers beendete den Spectral Scan.

VoIP

- Wenn ein LANCOM VoIP Router ein „INVITE" erhielt, dessen SDP-Teil zwei m-lines aufwies, antwortete das Gerät mit einem SIP-Paket, dessen SDP-Teil nur eine m-line aufwies. Dieses Verhalten war nicht RFC-konform und konnte im Zusammenspiel mit Fremdherstellern dazu führen, dass ein Anruf fehlschlug.
- Ausgehende, verschlüsselte Rufe zum Provider Telekom wurden abgelehnt, wenn für die SIP-Leitung die „Signalisierungs-Verschlüsselung" konfiguriert war. Auf das „INVITE" wurde ein „503 Service Unavailable" empfangen.
- Bei ausgehenden Rufen einer Nebenstelle wurde lediglich die Rufnummer der Zentrale übermittelt. Die P-Preferred Idenitity wurde hierbei nicht korrekt durch das SIP-Mapping gesetzt.
- Bei eingehenden Rufen an einem Telekom SIP-Trunk reichte der LANCOM Voice Call Manager den Parameter „user=phone" aus dem PAI-Header nicht an den SIP-Benutzer weiter.
- Wurde eine SIP-PBX-Leitung von einem LANCOM VoIP-Router auf eine vorgeschaltete O2-Box aufgebaut, so konnte es vorkommen, dass eingehende Anrufe vom LANCOM-Router mit der Meldung „Missing Mandatory Headers" abgelehnt wurden.
- Der LANCOM VoIP-Router hat SIP-Anrufe, welche durch einen Connection Timeout getrennt wurden, gelöscht. In der Folge wurde die Gegenstelle nicht mittels einer CANCEL-Nachricht informiert.

LCOS-Änderungen 10.12.0243 RU5 > 10.12.0292 RU6

Neue Features

- Bei einer Mobilfunknetz-Auswahl abhängig von der Signalqualität lässt sich nun eine Einschränkung auf erlaubte Mobilfunknetze (Blacklist) festlegen.
- Die Dienstlisten der Layer-7-Anwendungserkennung wurden aktualisiert.
- Die Geräte L-1302acn dual Wireless und L-1310acn dual Wireless signalisieren nun durch eine dauerhaft orange leuchtende Power-LED eine nicht ausreichende Stromversorgung via PoE und somit einen eingeschränkten WLAN-Betrieb.

Korrekturen / Anpassungen

Allgemein

- Cisco Kabelmodems der Typen 3208, 3212 und 3925 stellten aufgrund eines vom LANCOM nicht korrekt zusammengesetzten TCP-Pakets den Betrieb ein und konnten erst nach einem Neustart weiterbetrieben werden. Das falsch generierte TCP-Paket wird nun nicht mehr versendet.
- Ein über TR-069 (Carrier Device Management) und IPv6 administrierter Router konnte nach Übergabe der Konfiguration nicht mehr über die WAN-IPv6-Adresse angesprochen werden.
- Die Layer-7-Anwendungserkennung gab innerhalb von zwei Minuten einen massiven Anstieg des KByte-Counters für die Kategorie „Unknown“ wieder.
- Wenn die DTMF-Signalisierung sowohl beim SIP-Benutzer (Voice Call Manager > SIP-Benutzer) als auch auf der SIP-Leitung (Voice Call Manager > SIP-Leitungen > Erweitert) auf den Wert „Telefon-Events - Rückfall auf In-Band“ konfiguriert war, wurden Ereignisse bei einem eingehenden Anruf in RTP-Ereignisse transcodiert.
- Wenn bei einem mit dem Befehl „readscript -m -i“ erstellten Skript nach dem Parameter „flash No“ der Befehl „default -r“ eingefügt und der Befehl „flash Yes“ am Ende des Skripts entfernt wurde, kam es zu einem unerwarteten Neustart des Routers, wenn das modifizierte Skript mit dem Befehl „beginscript“ und Einfügen der Skriptdatei ausgeführt wurde.
- Wenn auf einem Gerät in einem Cluster-Szenario der zu synchronisierende Konfigurations-Snapshot größer als 1 MByte war, konnte ein Abgleich der Paramter via Config-Sync nicht vorgenommen werden.

VPN

- Wenn auf dem Initiator einer IKEv2-Verbindung bei konfiguriertem IKEv2-Loadbalancing ein Firmware-Update auf LCOS 10.12 SU3 durchgeführt wurde, konnte die VPN-Verbindung zum IKEv2-Loadbalancer nicht mehr aufgebaut werden.
- Der CA-Status des LANCOM 9100+ gab den Fehler „Maximum size of certificate list reached. No new certificates will be created." aus. Aus diesem Grund konnten keine neuen Zertifikate ausgestellt werden, da die Größe der Zertifikate durch die CA begrenzt wurde.
- Durch Optimierungen im GRE wurde die Routing-Performance von GRE-Tunneln (sowohl LAN-LAN als auch LAN-WAN) um etwa 15 % gesteigert.
- Bei Verwendung mehrerer Internet-Verbindungen und IKEv2-VPN-Verbindungen wurden Delete Notifications bei einem Wechsel der Internet-Verbindung über den falschen Internet-Zugang geroutet.

WLAN

- Bei der Verwendung von iPhones in einem von LANCOM LN-17xx Access Points ausgestrahlten WLAN-Netzwerk, konnte es zu Problemen bei der Übertragung von Daten kommen, welche nur durch kurzzeitiges Trennen der WLAN-Verbindung behoben werden konnten.
- Durch eine fehlerhafte Übertragung von CAPWAP-Paketen konnte es zu einem unvermittelten Neustart eines LANCOM WLAN-Controllers kommen.
- Es konnte in großen Netzwerk-Umgebungen bei Verwendung von P2P-Verbindungen, einer Client-Bridge oder Auto-WDS dazu kommen, dass ARP-Replies nicht übertragen werden konnten.
- Bei Access Points mit 802.11ac WLAN-Modul und aktivierter Stations-Überwachung konnte es bei einem hohen Datendurchsatz auf dem WLAN zu einer hohen Kanal-Last sowie einer hohen CPU-Last des Access Points kommen. In der Folge wurde der WLAN-Client vom WLAN dissoziiert.

VoIP

- 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 Standardwert „Reduktion der PMTU" eingestellt sein sollte.
- Bei der Fax-Übertragung per T.38 (Deutsche Telekom) wurde ein ReINVITE des LANCOM Routers seitens der Telekom zwar mit „200 OK" bestätigt, die Übertragung schlug aber dennoch fehl.
- Obwohl keine Call-Routing-Regel ausgeführt wurde, wurde eine Umsetzung der Rufnummer im FROM-Feld von „+" in „00" durchgeführt. Dies entsprach nicht dem E.164 Format.
- Bei Verwendung von Rufgruppen konnte es vorkommen, dass das „Busy-on-Busy"-Flag nicht korrekt übertragen wurde. In der Folge konnte es zu ungewollten Mehrfach-Anrufen kommen. Das „Busy-on-Busy"-Flag wird jetzt auch bei nicht aktivem „Busy-on-Busy" im Router übertragen.
- Nach einer Aktualisierung auf LCOS 10.12 RU5 konnte es vorkommen, dass Rufe an bestimmte Endgeräte (z.B. SNOM-Telefone) nicht mehr durchgestellt wurden.
- Es konnte sporadisch zu einem unvermittelten Neustart des VoIP-Routers kommen, wenn ein Analog-User eine irrtümlich gewählte Rufnummer während des Ruf-Aufbaus beendete.

LCOS-Änderungen 10.12.0242 RU4 > 10.12.0243 RU5

Korrekturen / Anpassungen

Allgemein

- Probleme beim Config-Reset wurden behoben.

LCOS-Änderungen 10.12.0147 SU3 > 10.12.0242 RU4

Neue Features

- Der RADIUS-Server unterstützt nun standardmäßig neben den Realm-Typen „Mail-Domain“ und „MS-Domain“ den Realm-Typ „MS-CompAuth“.
- Die Geräte LN-1700, LN-1702, LN-860 und LN-862 signalisieren nun durch eine dauerhaft orange leuchtende Power-LED eine nicht ausreichende Stromversorgung via PoE.
- Der VDSL-Linecode wurde für Geräte mit VDSL-Schnittstelle der Serien LANCOM 1781, 1783, 1784, R800, R88x sowie für den LANCOM 730VA aktualisiert.
- Verbindungsauf- und - abbauten sowie Verbindungsfehler von SIP-Leitungen werden nun im Syslog erfasst.
- Bei Neukonfigurationen sind nun die IPv4-Sperrrouten für RFC1918-Netze nicht mehr standardmäßig aktiviert.
- Durch die LMC verwaltete Geräte synchronisieren lokal vorgenommene Konfigurationsänderungen nun bei Bedarf mit der LMC.

Korrekturen / Anpassungen

Allgemein

- Es wurden keine Informationen zur WAN-Statistik per SNMP versendet, was z.B. im LANmonitor zu fehlenden Anzeigen führte.
- Der DHCP-Server sperrte bei der Prüfung, ob eine gewünschte Adresse frei ist, als bereits vergeben erkannte Adressen mit der maximalen Lease-Zeit. Diese Adressen werden nun nur noch für fünf Minuten gesperrt.
- Die Standard-Firewallregel für den Content Filter in der IPv6-Firewall erfasste alle Protokolle und alle Stationen zu allen Stationen.
- 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.
- In manchen Fällen wurden Routen mit der Einstellung „Sticky für RIP“ nicht korrekt über das RIP-Protokoll propagiert.
- In der LANCOM ARP-Implementierung wurde eine Prüfung eingebaut, bei welcher empfangene ARP-Pakete mit einer Absende-MAC-Adresse und gesetztem Group-Bit (Multi-/Broadcast) verworfen wurden. Dies konnte dazu führen, dass eine Layer-2-Kommunikation nicht funktionierte und z.B. ein Ping an einen lokalen Server scheiterte.
- Ein Portforwarding des Ports 500 (UDP) funktionierte in einigen Szenarien nicht wie erwartet.
- Wenn eine Konfiguration als Skript ausgelesen wurde, konnte diese nicht fehlerfrei zurückgeschrieben werden, da es zu Fehlermeldungen im Public Spot-Modul kam.
- Wenn der zu synchronisierende Konfigurations-Snapshot größer als 1 MByte war, konnte ein Abgleich der Parameter via Config-Sync nicht vorgenommen werden.
- Im OSPF besteht die Möglichkeit, statische Routen per Routen-Redistribution zu verteilen. Nach einem Neustart des LANCOM Routers ging die Route jedoch in der OSPF-Datenbank verloren und konnte somit nicht mehr über die LSAs verteilt werden.
- Wenn ein LANCOM Router eine Zeit-Anfrage (NTP via UDP) empfing, welche eine Checksum 0 aufwies, so wurde

diese vom internen Dienst des Routers abgelehnt.

- DHCPoE-basierte Internet-Verbindungen, welche eine zusätzliche Maskierungs-Adresse (Molo-Adresse) erhielten, nutzten diese Adresse nur bis zur Hälfte der DHCP-Lease-Time. Bei einem DHCP-Renew ging die zusätzliche IP-Adresse verloren und es wurde ab diesem Zeitpunkt die per DHCP erhaltene Adresse verwendet.

VPN

- Statisch konfigurierte Routen auf VPN-Tunneln werden nun von OSPF durch die Routen-Redistribution propagiert.
- 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.
- Wenn per WEBconfig ein weiterer Administrator-Account angelegt werden sollte, fehlten in der Konfigurationsoberfläche Felder zur Eingabe unterschiedlicher Parameter sowie Checkboxen zur Vergabe von Funktionsrechten.
- Bei einigen Browsern konnte die Konfigurationsoberfläche des WEBconfig „einfrieren“ und die CPU-Last des Routers auf 100% steigen wenn der Setup-Assistent „Einwahl-Zugang bereitstellen“ genutzt und die Option „VPN-Client mit benutzerdefinierten Parametern auswählen“ verwendet wurde.

WLAN

- Bei Geräten mit 802.11ac Wave1-WLAN-Modulen konnte es sporadisch zu einem unvermittelten Neustart kommen, welcher von einem fehlerhaften Reset des WLAN-Moduls verursacht wurde.
- EAPoL-Pakete für die 802.1X-Authentifizierung wurden vom Access Point nicht weitergeleitet, wenn auf den Geräten Protokoll-Filter (unter Wireless-LAN/Security/Protokolle) definiert waren, welche Pakete von Clients verwerfen sollten. Ein explizierter Allow-Filter für EAPoL-Pakete (Ethertype 888e) löste den Fehler auf.
- Nach einer Firmware-Aktualisierung auf LCOS 10.12 SU3 wurde bei Punkt-zu-Punkt-Verbindungen im LANmonitor kein Wert für „Senderate (zur Gegenstelle)“ mehr angezeigt.
- Die Spectral Scan-Funktion in WEBconfig ließ nach kurzer Zeit bei einigen Browsern die Browser-Registerkarte „einfrieren“. In der Folge wurden keine Spectral Scan-Daten mehr angezeigt.
- Wenn für eine Public Spot-Template-Seite kein „Template Cache“ aktiviert war, konnte dies dazu führen, dass z.B. die Login-Seite des Public Spots nach einiger Zeit nicht mehr aufgerufen werden konnte. Bei Geräten mit mehr als 128 MByte RAM ist der Template Cache nun per Default immer aktiv.
- Beim Aktivieren einer Public Spot Option auf einem LANCOM Gerät wurden die benötigten Datei-Ordner nicht im LCOS-Menübaum angelegt. Dies erfolgte erst nach einem manuellen Neustart des Gerätes.
- Nach einem Firmwareupdate auf LCOS 10.12 SU3 kam es in einigen Fällen dazu, dass eine zuvor problemlos funktionierende Punkt-zu-Punkt WLAN-Verbindung nicht mehr aufgebaut werden konnte. Dieses Verhalten trat nur in Verbindung mit aktiviertem Spanning-Tree-Protokoll (STP) auf.
- Nach einem Firmware-Update konnte es bei aktiviertem WLAN-Protokollfilter vorkommen, dass einige WLAN-Clients sich nicht verbinden konnten.

VoIP

- Bei Verwendung des LANCOM Routers als VoIP-Gateway konnten Bandbreitenreservierungen der Telefonie in

seltenen Fällen eine Blockierung der Internet-Kommunikation verursachen.

- Ein CANCEL-Requst, welcher während eines Rufaufbaus vom LANCOM Router empfangen wurde, wurde nicht an das Telefon weitergeleitet. In der Folge wurde der Ruf weiterhin am Telefon signalisert.
- 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.
- Wenn ein UnREGISTER-Paket unbeantwortet blieb, wurden anstelle eines normalen REGISTER-Pakets weitere UnREGISTER-Pakete gesendet, was bei einigen Providern dazu führte, dass eine SIP-Leitung nicht registriert werden konnte.
- Wenn Anrufe mit unterdrückter Rufnummer über Trunk-Leitungen gesendet wurden, welche eine SIP-ID im „FROM"-Header benötigten, so konnten diese Anrufe nicht durchgestellt werden.
- Wenn ein T.38-ReINVITE direkt mit einem „487 Request Terminated" beantwortet wurde, baute der LANCOM Router den Ruf nicht direkt ab, was dazu führte, dass keine weiteren Faxe mehr empfangen werden konnten.
- Anrufe, die von einem DECT-Benutzer (angebunden über die DECT-Basisstation 510) an einen SIP- oder ISDN-Benutzer vermitteln werden sollten, schlugen fehl. Die DECT-Basisstation fügte beim Vermitteln ein zweites (Proxy)-Authorization-Feld im SIP-Header hinzu, welches vom LANCOM Voice Call Manager nicht interpretiert werden konnte.
- Bei Ausfall der primären WAN-Verbindung wurden registrierte SIP-Leitungen nach dem Umschalten auf ein vorhandenes LTE-Backup nicht mehr verbunden.
- Die Tabelle für analoge Benutzer wurde in der LCOS-Version 10.12 REL von vier auf zwei reduziert, was dazu führte, das bei einem Firmware-Update der dritte und der vierte Benutzer gelöscht wurden.
- 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.
- 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.

LCOS-Änderungen 10.12.0146 RU2 > 10.12.0147 SU3

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 10.12.0084 SU1 > 10.12.0146 RU2

Neue Features

- Der Treiber für das IEEE 802.11ac-Wave1-WLAN-Modul der folgenden Produkte wurde aktualisiert:
  LN-630acn dual Wireless, LN-830acn dual Wireless,
  L-1310acn dual Wireless, L-1302acn dual Wireless,
  IAP-821, IAP-822,
  OAP-821, OAP-822, OAP-830
- vRouter-Lizenzen des Typs „vRouter 500“ können nun aktiviert werden.
- Zero-Touch-Provisionierung mit der LANCOM Management Cloud: LANCOM Router mit Ethernet-WAN-Port bauen im Auslieferungszustand eine DHCPoE-Verbindung über den WAN-Port auf und verbinden sich mit der LANCOM Management Cloud.

Korrekturen / Anpassungen

Allgemein

- Ein Schreiben der Konfiguration via LANconfig per TFTP oder serieller Schnittstelle war nicht möglich, wenn das LANCOM Gerät keine aktivierte Public Spot Option besaß.
- Ein Zurückschreiben der Konfiguration auf einem LANCOM Gerät ohne freigeschaltete Public Spot Option war über die serielle Schnittstelle nicht möglich.
- Beim LANCOM 1780EW-4G+ konnte eine konfigurierte WWAN-Verbindung (LTE oder UMTS) sporadisch nicht verwendet werden, weil das Mobilfunk-Modul keine IP-Adresse per DHCP mehr bezog.
- Auf Geräten vom Typ LANCOM 1780EW-4G+ konnte 2G (GPRS) als Fallback für Mobilfunkverbindungen konfiguriert werden, obwohl dieses Gerät es nicht unterstützt.
- Die LCOS-interne CA-Hierarchie, welche die Geräte-Zertifikate für HTTPS-Verbindungen auf das Gerät erstellt, war beim LANCOM 7100(+) VPN, 9100(+) VPN, WLC-4025+ und WLC-4100 fehlerhaft. Dies führte zu Geräte-Zertifikaten, welche vom Browser nicht akzeptiert wurden.
- Ein fehlgeschlagener SCEP-Request verhinderte das Ausführen weiterer SCEP-Requests, obwohl eine andere Zertifizierungsstelle angefragt werden sollte.
- Eine Verbindung zu einer DHCPoE-Gegenstelle konnte nicht aufgebaut werden, wenn das der Gegenstelle zugeordnete DSLoL-Interface einer Bridge-Gruppe zugeordnet war.
- 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.
- 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 mitgegeben werden.
- Im DHCP-Offer wurde einem BOOTP-Client der Server nicht übermittelt, welcher unter „Boot-Images“ eingetragen war.
- 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 einschließt.

- Es wurden Pakete, welche durch eine Firewall-Regel zurückgewiesen werden sollten, übertragen, 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.

VPN

- Es konnte sporadisch zu einem unvermittelten Neustart des Gerätes kommen, wenn der Zeitpunkt eines IPSec-Verbindungsabbaus mit dem Zustellen eines Datenpaketes, noch zugehörend zur abgebauten IPSec-Verbindung zusammenfiel.
- Es war nicht möglich, mehrere Dynamic VPN-Aushandlungen gleichzeitig auszuführen. Dies führte dazu, dass die zugehörigen VPN-Tunnel nicht aufgebaut werden konnten.

WLAN

- Eine in der Konfiguration hinterlegte Sendeleistungsreduktion auf dem IEEE 802.11ac-Modul wurde im Unterband 2 nicht berücksichtigt. Die Reduktion wurde auf den EIRP berechnet und nicht wie gewünscht auf die maximale Sendeleistung des Moduls.
- Die Funktion „Adaptive RF Optimization" wurde um die Nutzungs-Bewertung der Kanäle durch andere WLAN-Geräte erweitert.
- Der WPA-Rekeying Mechanismus funktionierte aufgrund einer fehlenden Rekeying-ID nicht ordnungsgemäß.

VoIP

- Eine SIP-Leitung konnte die Registrierung verlieren, wenn der DNS-Name des Registrars über einen DNS-Server aufgelöst wurde, der ein TTL=0 mitgeliefert hat.
- Das Setzen eines Anruf-Präfix auf einer SIP-Leitungs-Gegenstelle unter „Voice Call Manager > Leitungen > SIP-Leitungen > ..." führte zur Weitergabe der rufenden Nummer in einem ungültigen Format (z.B. 0+49), da die internationale Vorwahl von z.B. +49 nicht in 0049 geändert wurde.
- Wenn ein eingehender Voice-over-IP Anruf länger als 120 Sekunden signalisiert wurde, ohne angenommen zu werden, und dann vom Provider beendet wurde, verblieb der Ruf mit dem Status „Klingeln" in der Ruf-Liste.

LCOS-Änderungen 10.12.0082 Rel > 10.12.0084 SU1

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 10.12.0059 RC2 > 10.12.0082 Rel

Korrekturen / Anpassungen

Allgemein

- Nach einem Neustart des LANCOM Gerätes verblieben alle Ports im Status „disabled“, obwohl Spanning Tree aktiviert war.
- Eine per DHCP-Option zugewiesene LMC-Domäne wurde vom LANCOM Gerät (DHCP-Client) ignoriert.
- Eine ADSL-Verbindung mit der Encapsulation VC-MUX und einem transparenten Layer-2 (anstelle von PPPoE) konnte nicht erfolgreich aufgebaut werden.
- Nach Ablauf der Lease-Time wurde auf einer Internet-Gegenstelle mit dem Layer DHCPoEoV keine neue IP-Adresse bezogen und die Verbindung wurde kurzzeitig unterbrochen.
- 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.
- Wenn in der Netzwerk-Definition der LANCOM Management Cloud eine VLAN-ID eingetragen wurde, die gößer als 999 war, wurde diese Konfiguration nicht akzeptiert, obwohl VLAN-IDs bis 4094 in den Netzwerk-Definitionen erlaubt sind.
- Wenn ein NTP-Server im Netzwerk INTRANET konfiguriert war, so konnte die Konfiguration des Gerätes über LANconfig nach einer beliebigen Änderung nicht mehr zurückgeschrieben werden.
- Geroutete Multicasts (z.B. Videostream an DSL-1) wurden innerhalb einer Bridge-Gruppe (z.B. BRG-1) am IGMP-Snooping vorbei auf das Interface LAN-1 und, sobald ein Client im WLAN eingebucht war, auch auf WLAN-1 gebridged. Dies führte dazu, dass das WLAN mit Multicast-Paketen „überflutet“ wurde und die WLAN-Kanallast derart anstieg. dass die WLAN-Verbindung nicht performant genug war.
- 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.
- In einem EoGRE-Tunnel, dem unter Schnittstellen -> LAN -> Port-Tabelle keiner Bridge-Gruppe zugewiesen wurde, wurden keine Daten übertragen.

WLAN

- Per AutoWDS konnte keine Punkt-zu-Punkt Verbindung zwischen LANCOM Access Points hergestellt werden. Die für AutoWDS eingetragenen Access Points wurden zwar in der entsprechenden SSID angezeigt (im LANmonitor), eine Verbindung kam jedoch nicht zustande.
- Clients, welche am LANCOM Public Spot initial angemeldet waren, konnten keine Verbindung zum WAN herstellen, da die DNS-Anfragen der initialen Domain nicht an ein vorgeschaltetes Gerät (welches den WAN-Zugang bereitstellte) weitergeleitet wurden.
- Beim Auslesen der Konfiguration eines LANCOM WLAN-Controller per LANconfig wurde das Wireless-IDS-Profil „Default“ nicht mit ausgelesen. In der Folge konnte die Konfiguration nicht in den LANCOM WLAN-Controller zurückgeschrieben werden.

VoIP

- 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“.
- Wenn im LANCOM Voice Call Manager in den Einstellungen eines Benutzers (Voice Call Manager > Benutzer > Benutzer Einstellungen) die Funktion „Zweitanruf unterdrücken (Busy-on-Busy)“ aktiviert war, wurden dem jeweiligen Benutzer keine Anrufe zugestellt.

VPN & Routing

- Eine IKEv2-Verbindung mit einen Digital-Signature-Profil „RSASSA-PSS mit SHA-384 und SHA-512“ konnte nicht aufgebaut werden.
- 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.
- Auf einer IKEv2-Verbindung, welche über IKEv2-RADIUS authentifiziert wurde, wurden nach mehr als 24 Stunden keine ausgehenden Daten mehr übertragen. Die Lifetimes wurden vom LANCOM Router in der RADIUS-Authentifizierung nicht korrekt übernommen.
- Bei einer für den LANCOM Advanced VPN Client angelegten IKEv2-Gegenstelle mit dem Verschlüsselungsverfahren AES-GCM wurden im aufgebauten VPN-Tunnel nur UDP- und ICMP-Pakete übertragen. TCP-Verbindungen funktionierten hingegen nicht (SSH, HTTPS etc.).
- Wenn in der Komandozeile eines LANCOM Routers der Befehl „show vpn“ eingegeben wurde, zeigte die Ausgabe VPN-Regeln von konfigurierten IKEv2-Verbindungen als IKEv1-Regeln an.
- 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.

- Dynamic VPN-Verbindungen (IKEv1 über UDP) zwischen zwei LANCOM Routern, bei der die dynamische Seite mit einer privaten IP-Adresse auf der Internet-Verbindung (hinter einem NAT-Router) betrieben wurden, konnten nicht aufgebaut werden. Eine Dynamic VPN-Verbindung über ICMP funktionierte.

LCOS-Änderungen 10.12.0041 RC1 > 10.12.0059 RC2

Neue Features

Allgemein

- Für den COM-Port-Server kann nun die Erreichbarkeit über WAN-Verbindungen konfiguriert werden.
- Dynamisch erzeugte VLAN-Mitgliedschaften können nun auf der CLI mit dem Befehl „show vlan“ angezeigt werden.
- Die Dienstlisten der Layer-7-Anwendungserkennung wurden aktualisiert.
- Die Layer-7-Anwendungserkennung unterstützt nun die Erkennung von QUIC-Sessions.
- Unterstützung für Ethernet OAM nach 1TR112

WLAN

- Der Treiber für das IEEE 802.11ac Wave1-WLAN-Modul der folgenden Produkte wurde aktualisiert:
  LN-630acn dual Wireless, LN-822acn dual Wireless, LN-830acn dual Wireless, LN-830E Wireless,
  L-1310acn dual Wireless, L-1302acn dual Wireless,
  IAP-821, IAP-822,
  OAP-821, OAP-822, OAP-830

VoIP

- „Busy-on-Busy“ ist nun für Rufgruppen konfigurierbar.

Korrekturen / Anpassungen

Allgemein

- Im Content Filter war die Kategorie „Cloud-Anwendungen“ in den drei voreingestellten Default-Profilen als „Verboten“ definiert. Dies wurde nun auf „Erlaubt“ geändert.
- Die Uhrzeit, welche die LANCOM Management Cloud (LMC) periodisch setzt, wurde von einem LANCOM WLAN-Controller im Netzwerk überschrieben, wenn dieser seine Uhrzeit an einen von ihm verwalteten LANCOM Access Point meldete.
- In der Konfigurationsoberfläche des LANCOM 1783VAW fehlte die Möglichkeit zur Konfiguration der LACP-Schnittstellen „Bundle-1“ und „Bundle-2“.

VPN & Routing

- Wenn auf einem LANCOM Router VPN-Verbindungen terminiert wurden, die eine AES-GCM- Verschlüsselung verwendeten, so fehlten in der LCOS-Tabelle /Status/VPN/ESP die Werte in den Spalten „Crypt-Alg“ und „Hash-Alg“.
- Wenn auf einem LANCOM Router ausschließlich Default-Routen mit einem Routing-Tag ungleich 0 definiert waren, konnten IKEv2-Verbindungen nicht aufgebaut werden, wenn der IKEv2-Peer nicht anhand der IP-Adresse erkannt wurde.
- 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 VPN-Gegenstelle ein oder mehrere N:N-NAT-Einträge hinterlegt waren, welche die übergeordnete IPSec-Regel einschloss.

WLAN

- Das Länderprofil „Australien“ wurde korrigiert.
- Bei Verwendung des Client-Bridge-Modus auf IEEE 802.11ac-fähigen WLAN-Modulen werden ARP-Pakete nun zuverlässig übertragen.
- 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.
- Das IEEE 802.11ac-Funkmodul eines LANCOM Access Point sendete im 2,4-GHz-Band sowohl im Modus 802.11gn/mixed als auch im Greenfield-Modus Beacons mit einer Datenrate von 1 MBit/s. Dies führte dazu, dass die Beacons auch auf einem 802.11b-Client sichtbar waren, obwohl der 802.11b-Modus in der Konfiguration des Access Points nicht ausgewählt war.
- Für die Public Spot-Loginmethode „Login nach Einverständniserklärung“ wird nun auf der Statusseite kein Logout-Link mehr angezeigt.
- Auf der Login-Seite des Public Spot-Gateways konnte 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.
- 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 ebenfalls die Public Spot-SSID ausstrahlte, wurde der Eintrag für einen Client, der beim Roaming vom Router auf den Access Point wechselte, aus der Auto-Re-Login-Tabelle gelöscht. Dies führte dazu, dass ein erneutes Login am Public Spot erforderlich war.
- Bei einem LANCOM WLAN-Controller wurde nach Durchführung einer Funkfeldoptimierung im LANmonitor ein negativer Wert für verwaltete Access Points angezeigt.

VoIP

- Beim Betrieb einer VoIP-Leitung (SIP-Trunk) über einen BNG-Anschluss als Internetverbindung und Nutzung einer ISDN-TK-Anlage hinter einem LANCOM VoIP-Router konnte es gelegentlich zu einseitiger Sprachübertragung kommen. Der interne ISDN-Teilnehmer hörte den externen Teilnehmer nicht mehr.
- Telefonate von einer internen SIP-TK-Anlage über einen LANCOM VoIP Router an eine SIP-Trunk-Leitung des Providers „Deutsche Telefon“ wurden nach ca. 15 Minuten getrennt.
- Wenn im Menü „Voice-Call-Manager --> Erweitert“ ein oder mehrere Präfixe für interne Anrufe konfiguriert wurden, so wurde das konfigurierte Präfix bei der Quell-Rufnummer nicht angehängt. In der Folge konnte ein ausgehender Anruf nicht durchgeführt werden.
- Nach erfolgreicher Registrierung einer SIP-Leitung über IPv6 funktionierten eingehende Gespräche nicht, da die INVITE-Pakete von der Firewall des LANCOM VoIP-Routers mit einem „ICMP Port Unreachable“ beantwortet wurden, obwohl eine vorhandene Inbound Firewall-Regel für den SIP-Server vorhanden war.

LCOS 10.12.0041 RC1

Geräte mit LCOS 10.12 RC1 können derzeit nicht über die LANCOM Management Cloud konfiguriert oder verwaltet werden.

Neue Features

Allgemein

- LACP - virtuelle Bündelung von Ethernet-Ports für hohe Ausfallsicherheit
- Public Spot-Unterstützung für den LANCOM vRouter
- Kommando zum Umschalten der Firmware mit anschließendem, automatischem Neustart
- Dateiimport per Copy & Paste
- Smart Ticket/SMS - Whitelist für Rufnummern-Vorwahlen
- Entfall des Ports 8080 bei WEBconfig und Public Spot
- Erweiterung des Content-Filters um weitere Kategorien
- IPv6-Unterstützung für den Content-Filter

VPN & Routing

- IKEv2 Load Balancer für das Load Balancing eingehender VPN-Verbindungen
- Frei konfigurierbare DHCPv6-Optionen
- OSPFv2
- OCSP-Prüfung im TLS/Rollout-Agent
- Schaltbare Nicht-HTTPS-Kommunikation über Port 443 im Content-Filter
- Unterstützung von AES-GCM bei IKEv2
- Unterstützung der elliptischen Diffie-Hellmann-Gruppen (ECDH) 19, 20 und 21 sowie der ECC Brainpool-Kurven 28, 29 und 30 bei IKEv2
- Unterstützung für RADIUS CoA bei IKEv2
- Erweiterte VPN-Backup-Mechanismen für höchste Verfügbarkeit im VPN
- Unterstützung für TACACS Shell-Autorisierung
- Variablen für IPv6-LAN-Adresse und Präfix in der Aktionstabelle
- ICMPv4 und ICMPv6-Rate-Limiting
- Unterstützung von MD5 im NTP-Client und Server
- NTP-Server pro ARF-Netz schaltbar

WLAN

- Multicast > Unicast-Umwandlung für ruckelfreies IPTV im WLAN
- Die Menüs zur Public Spot-Konfiguration sind ab sofort grundsätzlich im LCOS vorhanden, können aber erst nach erfolgreicher Aktivierung der Public Spot-Option verwendet werden.
- Erreichbarkeitsprüfung für RADIUS-Server im 802.1X
- 802.11ac Wave 2 Features via WLC konfigurierbar
- Koordinierte Wireless ePaper-Kanalwahl

VoIP

- Das SIP User-ID-Feld ist nun schaltbar
- Overlap Dialing ermöglicht schnelleren Verbindungsaufbau

Korrekturen / Anpassungen

Allgemein

- Wenn die Gültigkeit eines RA-Zertifikates vor der Gültigkeit des CA-Zertifikats ablief, aktualisierte der SCEP-Client das RA-Zertifikat nicht.
- Wenn die Spanning Tree-Funktion per LANconfig auf LANCOM Access Points aktiviert wurde, wurde diese Änderung nicht korrekt zurückgeschrieben, sodass Spanning Tree nach dem Zurückschreiben der Konfiguration weiterhin deaktiviert war.
- Beim Hochladen einer vRouter-Konfiguration per WEBconfig wurden die Konfigurationsparameter nur dann vollständig übernommen, wenn beim vRouter nach dem Hochladen der Konfiguration ein Warmstart ausgeführt wurde.
- Bei Verwendung eines Backup RADIUS-Servers zur Geräte-Authentifizierung wurde das Login zuerst auf dem Backup-Server statt auf dem primären RADIUS-Server geprüft.
- Wenn in der Zeit des DHCP-Bezugs der DHCP-Client neu startete, konnte es vorkommen, dass der LANCOM DHCP-Server diesem Client nach dem Neustart keine IP-Adresse mehr zuwies, und in der Trace-Ausgabe zu DHCP die Meldung „ARP in progress“ erschien.
- Proxy-ARP für die Kommunikation zwischen identischen, vom LANCOM verwalteten IP-Netzwerken wurde nicht ausgeführt.
- Bei einer Internet-Verbindung, die als DS-Lite angelegt war, konnte es vorkommen, dass der LANCOM für IPv6-Pakete nicht seine IPv6-WAN-Adresse, sondern seine IPv6-LAN-Adresse als Absender verwendete.
- Der LCOS CRL-Client fragte alle Typen von CRL-Distribution-Points ab, obwohl der CRL-Client nur den Typ HTTP unterstützt.
- Die Tabelle „Setup/DNS/DNS-Destinations“ (LANconfig: IPv4 -> DNS -> Weiterleitungen) akzeptierte für den Parameter „Rtg-tag“ (Routing-Tag) nur Werte kleiner oder gleich 999.
- Im LANCOM vRouter fehlten im Setupmenü „/Setup/WAN“ die Tabellen zur Konfiguration von Backup und Accounting.

- Wenn auf der Kommandozeile der Befehl „show script“ eingegeben wurde, enthielt die Ausgabe keine Session-IDs mehr. Laufende Skripte konnten daher nicht mehr mit dem Befehl „killscript <Session-ID>“ gestoppt werden.
- Im LANCOM vRouter fehlte das Setupmenü (/Setup/WAN/RADIUS) für die Authentifizierung über einen externen RADIUS-Server.
- Eine xDSL-Verbindung wurde nicht sofort abgebaut, wenn die dazugehörige DSL-Gegenstelle per Script aus der Konfiguration gelöst wurde.
- Es konnte zu einem unvermittelten Neustart des Gerätes nach Aufruf des benutzerdefinierten Rollout-Assistenten kommen, wenn im benutzerdefinierten Rollout-Assistenten für eine Auswahl-Liste mehr Werte (item_value) als Text (item_text) definiert waren.

VPN

- Sollte eine DHCP-Anfrage über einen VPN-Tunnel weitergeleitet werden, der über den Config-Mode eine IP-Adresse erhielt, wurde die Config-Mode Adresse auch als GI-Adresse im DHCP-Header eingetragen.
- Wenn eine bestehende VPN-Verbindung mit einer Delete-Information abgebaut wurde, war im VPN-Debug-Trace keine Information über den Auslösegrund enthalten.
- Im WEBconfig-Konfigurationsdialog für die IKEv2-Rekeying-Parameter (Konfiguration -> VPN -> IKEv2/IPSec -> Gültigkeitsdauer) fehlten Namensbezeichnungen bei zwei konfigurierbaren Parametern.
- Wurde eine IKE-Verbindung, die zwischen einem vRouter und einem VPN-Router aufgebaut werden sollte, per DPD überwacht, erfolgte immer wieder ein Verbindungsabbruch auf Grund eines DPD Timeout. Das DPD wurde auf dem LANCOM vRouter nicht korrekt ausgeführt.

WLAN

- Der Trigger zur Re-Initialisierung des SCEP-Clients konnte ins Leere laufen, wenn sich der Client gerade in der Initialisierung befand.
- Der Wert zur Begrenzung des Datenvolumens für automatisch erzeugte Public-Spot Benutzer im Pfad „/Setup/Public-Spot-Module/Authentication-Modules/User-Template/Volume-Budget“ war auf einen Maximalwert von 4.000 MByte begrenzt.
- Beim Erstellen von Public-Spot-Benutzern per HTTP-Befehl wurde ein in der URL angegebener Kommentar nicht in das erstellte Benutzerprofil übernommen.
- Es konnte zu einem unvermittelten Neustart des Gerätes kommen, wenn der Access Point für die WLAN-Clients einen WLC-Tunnel (CAPWAP-Datentunnel) bereitstellte und einem WLAN-Client ein ICMP-Paket „Fragmentation needed“ zustellen wollte, da das vom WLAN-Client empfangene Datenpaket zu groß für den CAPWAP-Datentunnel war.

VoIP

- 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.
- Bei einem ausgehenden SIP-Anruf wandelte der LANCOM Voice Call Manager eine Landesvorwahl, welche mit einem „+" beginnt (z.B. +492405123456) nicht in das Format 0049 um, was zur Folge hatte, dass eine ISDN-Telefonanlage die Rufnummer nicht auswerten und der Anruf nicht durchgeführt werden konnte.
- Wenn auf der Konsole die SIP-Leitung mit dem Befehl „do /other/manual-dialing/disconnect <Verbindung>" getrennt wurde, dann wurde der LANCOM Voice Call Manager nicht über das Trennen der Verbindung informiert, was zur Folge hatte, das die Leitungen, die diese ‚Verbindung' nutzen, nach wie vor als registriert angezeigt wurden.
- 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 ein VoIP-Provider auf die De-Registrierung einer SIP-Leitung mit der Fehlermeldung „400 Bad Request" antwortete, konnte der LANCOM Voice Call Manager diese Fehlermeldung nicht interpretieren, was dazu führte, dass die De-Registrierung der SIP-Leitung ständig wiederholt wurde und keine Neuregistrierung stattfinden konnte.
- Sollte eine Rufgruppe als Backup-Leitung, z.B. für eine Verbindung zu einer TK-Anlage, verwendet werden, so funktionierte dieser Eintrag nicht.
- 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.
- Eine SIP-Leitung, welche mittels OPTIONS-Pakete registriert wurde, wurde vom SIP-ALG nicht als registrierte Leitung interpretiert, demzufolge eingehende Calls (INVITE-Pakete) nicht korrekt zugeordnet wurden.
- Aufgrund des Parameters „transport=UDP" im Contact-Header eines SIP-Paketes verloren einige lokale SIP-Clients nach wenigen Minuten die Registrierung zum LANCOM VoIP-Router.
- Bei LANCOM VoIP-Routern trat ein sporadisches Problem bei Anrufen auf, an denen die LANCOM 510 DECT Basisstation beteiligt war. Wenn ein externer Ruf auf einer SIP-Leitung am LANCOM VoIP-Router ankam und intern an einem Handset des LANCOM N510 DECT angenommen wurde, hörte der Anrufer den internen Teilnehmer, der interne Teilnehmer aber den Anrufer nicht.
- Es konnte zu einem unvermittelten Neustart des Gerätes kommen, wenn das empfangene OK-Paket auf einer SIP-Leitung im CONTACT-Header keinen Expires-Wert beinhaltete.
- Es konnte sporadisch eine einseitige Verständigung auftreten, wenn ein eingehender Call über eine SIP-Leitung vom LANCOM VoIP-Router intern auf mehr als 2 Interfaces (ISDN- und Analog-Schnittstellen) signalisiert wurde.
- Ein SETUP, welches auf dem ISDN empfangen wurde und eine Zielrufnummer vom Typ „National Number" enthielt, wurde vom Call-Routing nicht um Nullen ergänzt, wie es z.B. bei Nummern vom Typ „International Number" der Fall ist. In der Folge scheiterte das Call-Routing mit Service-Nummern.

- Nachdem ein analoger Anruf beendet wurde, blieb dieser in seltenen Fällen in der Call Counter-Tabelle des LANCOM VoIP-Routers als Eintrag erhalten.
- Ein Linphone SIP-Client wurde bei der Anmeldung am Voice Call Manager (VCM) aufgrund von für den Client spezifischen Parametern innerhalb der Anmeldung abgelehnt.

3. Wichtige 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.

Allgemeine Hinweise

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/lcos/lifecycle-management/produkttabellen/

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 erst nach einem internen Test in der Kundenumgebung aktualisiert werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

Gerätespezifische Empfehlungen

LANCOM 178x-4G:

Um Verzögerungen beim Aufbau von Mobilfunk-Verbindungen (z.B. im Backup-Fall) zu vermeiden, wird empfohlen, im verbauten LTE-Mobilfunk Modem des Typs Sierra MC-7710 den LTE-Modem-Treiber der Version 3.5.24 einzusetzen. Beachten Sie dazu bitte auch den folgenden Knowledge Base-Artikel: Link

Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umstän-den 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, insbesonde-re die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.