LANCOM Release Notes

LCOS

10.50 RU5

Copyright © 2002-2022 LANCOM Systems GmbH, Würselen (Germany)

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

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

09.02.2022, CBuersch

Inhaltsübersicht

1. Einleitung **2**
2. Gerätespezifische Kompatibilität zu LCOS 10.50 **3**
3. Hinweise zu LCOS 10.50 **3**
Informationen zu Werkseinstellungen 3
4. Feature-Übersicht LCOS 10.50 **4**
4.1 Feature-Highlights 10.50 **4**
Performance-Upgrade für den LANCOM ISG-8000 4
Schnelles Failover für höchste Betriebssicherheit 4
4.2 Weitere Features LCOS 10.50 **5**
Erweiterung der IPv6-Funktionalität 5
Plattformerweiterung für den LANCOM vRouter 5
5. Historie LCOS 10.50 **6**
LCOS-Änderungen 10.50.0619 RU5 6
LCOS-Änderungen 10.50.0530 RU4 8
LCOS-Änderungen 10.50.0434 RU3 10
LCOS-Änderungen 10.50.0331 RU2 12
LCOS-Änderungen 10.50.0235 RU1 13
LCOS-Änderungen 10.50.0145 Rel 15
LCOS-Änderungen 10.50.0129 RC3 17
LCOS-Änderungen 10.50.0115 RC2 18
LCOS-Änderungen 10.50.0091 RC1 18

LANCOM Systems

6. Allgemeine Hinweise **20**
Haftungsausschluss 20
Sichern der aktuellen Konfiguration 20
Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes 20

1. Einleitung

Alle Mitglieder der LANCOM Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.50 RU5 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 10.50

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/

Die Unterstützung für die folgenden Geräte entfällt ab LCOS 10.50:

- LANCOM 1631E
- LANCOM 1781-4G
- LANCOM 1781A
- LANCOM 1781AW
- LANCOM 1781VA-4G
- LANCOM 730-4G
- LANCOM 7100+
- LANCOM 9100+
- LANCOM IAP-4G
- LANCOM L-151
- LANCOM L-151E
- LANCOM L-320 R2
- LANCOM L-330
- LANCOM WLC-4025+
- LANCOM WLC-4100

3. Hinweise zu LCOS 10.50

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 10.50

4.1 Feature-Highlights 10.50

Performance-Upgrade für den LANCOM ISG-8000

In großen SD-WAN- oder Standortvernetzungsszenarien mit einer Vielzahl an IPSec-VPN-Kanälen und hohem Datenaufkommen ist der Einsatz des Central Site VPN-Gateways LANCOM ISG-8000 nun noch effizienter. Durch die intelligente Verteilung der Datenlast auf mehrere Kerne (Multicore) wird die Gesamtperformance der VPN-Verbindungen auf 10 GBit/s erhöht. So können bei der Nutzung vieler VPN-Kanäle deutlich mehr Daten in kürzerer Zeit ausgetauscht werden.

Schnelles Failover für höchste Betriebssicherheit

In Infrastrukturen mit Anforderungen an höchste Betriebssicherheit sind schnelle Failover-Zeiten essenziell wichtig. Bei Einsatz von Dynamic Path Selection (DPS) oder BGP gelingt das Umschalten von einer IPSec-VPN-Verbindung zur anderen nun in weniger als einer Sekunde. Somit führt in einem Active-Active-Betrieb der Ausfall einer Verbindung zu keiner merklichen Downtime, beispielsweise bei geschäftskritischen Prozessen wie Zahlungsvorgängen mit EC-Cash-Terminals.

4.2 Weitere Features LCOS 10.50

Erweiterung der IPv6-Funktionalität

Profitieren Sie jetzt von noch mehr Zukunftsfähigkeit Ihrer IPv6-Standortvernetzung: Ab LCOS 10.50 RC1 werden Funktionen wie 464XLAT bei IPv6-only im Mobilfunk, NAT bei IPv6 (NPTv6), Load Balancing mit IPv6 sowie IPv6-Polling unterstützt.

Plattformerweiterung für den LANCOM vRouter

Für einen noch flexibleren Einsatz unterstützt der LANCOM vRouter neben den Hypervisor-Plattformen Hyper-V, ESXi und Azure jetzt auch KVM (Kernel-based Virtual Machine).

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 5 „Historie LCOS 10.50“.

5. Historie LCOS 10.50

LCOS-Änderungen 10.50.0619 RU5

Neue Features

- Der USB-Drucker-Server ist nach einem Geräte-Reset im Default deaktiviert.
- Der Netzwerkname kann nun bei den Aktionstabellenvariablen für IPv6 LAN-Adresse und LAN-Präfix (%x und %y) angegeben werden.

Korrekturen / Anpassungen

Allgemein

- Nach einer Reinitialisierung des WWAN-Modems beim LANCOM 1790VA-4G+ mit dem Befehl ‚do /status/usb/reinit' war das Modem ohne Funktion. Nur mit einem kompletten Neustart des Routers konnte die Funktionalität des WWAN-Modems wieder hergestellt werden.
- Da die SNMP EngineID bei LANCOM Geräten im Enterprise-ID-Format ausgelesen wird, war diese bei einer Abfrage über eine OID um 1 Byte zu kurz, weshalb zwei Zeichen fehlten. In der Folge meldeten die Geräte, dass sie die gleiche SNMP EngineID verwenden.
- Wenn ein NTP-Netzwerk für den NTP-Server per Konsole eingetragen wurde, fand dieses keine Anwendung. Dies führte dazu, dass Geräte in diesem Netzwerk keine Zeit von diesem NTP-Server beziehen konnten. Im NTP-Trace wurde die Fehlermeldung „LAN-Request received, but sender is not in Networklist" ausgegeben.
- Bei Verbindungsaufbau einer VPN-Verbindung über das 5G-Modul (WWAN) eines LANCOM 1926VAG-5G oder 1900EF-5G war keine Kommunikation über die VPN-Verbindung möglich.
- Ein DynDNS-Abgleich über die Aktionstabelle per IPv6 war nicht mit einem statischen Präfix möglich. Weiterhin funktionierte der DynDNS-Abgleich nur für das Netzwerk INTRANET, nicht aber für andere Netzwerke.
- Auf einem vRouter sowie auf dem LANCOM ISG-8000 wurde die ‚Checksum Offloading Info' immer hinzugefügt, auch wenn dies nicht erforderlich war. Dies konnte bei mit einem VLAN-Tag versehenen Paketen dazu führen, dass diese nicht übertragen werden konnten.
- Wenn ein Access Point oder Router mit mindestens zwei Netzwerken verwendet und die IP-Adresse in diesen Netzwerken per DHCP bezogen wurde, konnte es vorkommen, dass der HTTP-Client für den Verbindungsaufbau zur LMC statt der LMC Loopback-Adresse die undefinierte IP-Adresse 0.0.0.0 verwendete. Dies führte dazu, dass für die Verbindung zur LMC eine IP-Adresse aus einem anderen Netzwerk verwendet wurde und die Verbindung zur LMC immer wieder abbrach.
- In LCOS 10.42 wurde die Mobilfunk-Verbindungshistorie im Pfad ‚/Status/Modem-Mobile/History' von 100 auf 512 Einträge erweitert. Nach einem Firmware-Update auf eine entsprechende Version wurde die Tabelle nicht korrekt auf die neue Größe konvertiert und daher weiterhin eine Tabelle mit 100 Einträgen verwendet. Wenn mehr als 100 Einträge geschrieben wurden, führte dies zu einem unvermittelten Neustart des Routers.

VPN

- Für ein Interface mit noch nicht ausgehandelter MTU wurde ein Standard-Wert von 1280 Bytes verwendet. Da die Anpassung an die MTU nicht korrekt funktionierte, wurde weiterhin der Standard-Wert von 1280 Bytes verwendet. Dies führte dazu, dass größere Pakete mit gesetztem ‚Don't fragment' Flag über eine VPN-Verbindung nicht übertragen werden konnten und die Kommunikation somit stark gestört oder nur sehr langsam möglich war.

VoIP

- Wenn der LANCOM VoIP-Router einen Anruf empfing, der optionale Angaben zur verwendeten Bandbreite der Session enthielt, kopierte er diese Zeilen doppelt in die Antwort „200 OK", welche er beim Annehmen des Anrufs sendete. In der Folge kam ein eingehender Anruf nicht zustande.
- Bei der Verwendung von SNOM DECT-Endgeräten konnte es vorkommen, dass diese sich nicht mehr am LANCOM Router registrieren konnten, da Geräte die ‚Contact URI' bei jedem Registrierungsvorgang veränderten und die im REGISTER gesendete Änderung nicht in der gespeicherten Binding-Information des LANCOM Routers geändert wurde.
- Bei einem ‚Vodafone Anlagenanschluss Plus' konnte es bei eingehenden Anrufen vorkommen, dass die ‚Halten'-Funktion nicht ausgeführt werden konnte, da im RE-INVITE des Voice Call Managers keine P-Preferred-Identity (PPI) enthalten war.
- Der Voice Call Manager überprüfte seinen DNS-Cache alle 5 Sekunden auf abgelaufene SRV-Records (TTL = 0) und löschte diese anschließend. Traf die Antwort auf eine DNS-Anfrage erst nach Löschung des entsprechenden SRV-Records am Voice Call Manager ein, wurde die SIP-Leitung abgebaut und im Syslog die Meldung „generic failure" ausgegeben.

  Abgelaufene SRV-Records werden jetzt erst nach zweimaliger Überprüfung (insgesamt 10 Sekunden) aus dem DNS-Cache entfernt. Weiterhin wird die SIP-Leitung nicht abgebaut, solange die vorhandene Verbindung zum SIP-Server funktioniert.
- Wenn der SIP-Provider eine Änderung der Priorität der SIP-Server in einem SRV-Response ankündigte, wurde die SIP-Leitung abgebaut und im Syslog die Meldung „generic failure" ausgegeben.

  Die SIP-Verbindung wird jetzt nur noch dann ab- und neu aufgebaut, wenn die IP-Adresse des aktuell verwendeten SIP-Servers nicht mehr der IP-Adresse des höchst-priorisierten Servers entspricht. In diesem Fall wird im Syslog die Fehlermeldung „server order changed" ausgegeben.

LCOS-Änderungen 10.50.0530 RU4

Neue Features

- Für den 802.1X-Authenticator für LAN-Verbindungen lässt sich nun ein getrennter RADIUS-Server für den MAC-Authentisierungs-Bypass angeben.

Korrekturen / Anpassungen

Allgemein

- Eine Änderung der Übertragungs-Betriebsart in der WWAN-Konfiguration eines LANCOM 5G-Routers hatte keine Auswirkung. Es wurden immer alle möglichen Betriebsarten verwendet.
- Wenn der PPTP-, PPPoE- oder der L2TP-Server aktiv war und gleichzeitig der Fernzugriff auf den Router erlaubt wurde, kam es bei einem Verbindungsaufbau-Versuch auf den Router unter Verwendung des Benutzernamens ‚admin' zu einem unvermittelten Neustart, welcher durch das Schreiben des Event-Logs ausgelöst wurde.
- Beim Aufruf von HTTPS-Webseiten durch das Feature ‚Dynamic Path Selection' verwarf der HTTP-Client im Router die HTTPS-Sessions nicht und gab auch den Speicher nicht wieder frei. Dies führte nach einiger Laufzeit zu einem unvermittelten Neustart des Routers, wenn kein freier Speicher mehr zur Verfügung stand.
- In Einzelfällen konnte es zu einem unvermittelten Neustart des Routers kommen, wenn eine interne IPSec-Tabelle noch nicht korrekt initialisiert war und ein IPSec-Paket empfangen wurde.
- Nach Anpassung der Schlüssellänge einer bestehenden Zertifizierungsstelle (CA) konnte diese anschließend nicht neu initialisiert werden, da aufgrund der unterschiedlichen Schlüssellänge die CA nicht gestartet werden konnte.
- Das WEBconfig- bzw. TLS-Geräte-Zertifikat eines mit LCOS betriebenen LANCOM Gerätes wurde über das Ablaufdatum im Jahr 2024 hinaus nicht automatisch vom Gerät verlängert.

WLAN

- Bei einem LANCOM ISG-8000 mit aktivierter Public Spot-Option lag die maximale Anzahl der unterstützen Public Spot-Benutzer anstatt der unbegrenzten Benutzeranzahl (empfohlen werden maximal 2500 Nutzer) bei 128 Benutzern.
- Nach der Durchführung eines Umgebungs-Scans zur Erkennung von Rogue Access Points verblieb das jeweilige WLAN-Modul im Scan-Modus. In der Folge konnte der normale WLAN-Betrieb auf dem Modul nicht verwendet werden.
- Bei Verwendung eines WLAN-Interfaces im P2P-Modus verwendet dieses als BSSID die MAC-Adresse der WLAN-Karte, und den logischen WLAN-Interfaces werden lokale MAC-Adressen als BSSID zugewiesen.
  Wenn die P2P-Konfiguration per Addin-Skript über die LMC ausgerollt wurde, konnten die Aktionen für die Zuweisung der MAC-Adressen nicht korrekt initiiert werden und somit erhielten das P2P-Interface und die weiteren logischen WLAN-Interfaces die gleiche BSSID. Dies führte zu einem unvermittelten Neustart des Access Points. Weiterhin wurde die P2P-Konfiguration nicht übernommen.

VoIP

- Das ‚#'-Zeichen wird im ASCII-Zeichensatz mit ‚%23' codiert. Wenn in einer Call-Route eine Filterung der gerufenen Nummer z.B. mit ‚#21#' verwendet wurde, im ‚To'-Header des entsprechenden INVITE jedoch die Zeichenfolge ‚%2321%23' angegeben war, wurde das Invite falsch bearbeitet und ein Anruf kam nicht zustande, da die Zeichenfolge ‚%23' nicht als nur ein Sonderzeichen, sondern als drei Zeichen behandelt wurde. Im LANCOM Router erfolgt daher nun immer zunächst eine Umwandlung von ‚%23' in ‚#' und später (aus Kompatibilitätsgründen) zurück zu ‚%23'.
- Der Voice Call Manager handelt mit dem SIP-Provider einen Wert für die Aktualisierung der Registrierung (Min-Expires) aus und verwendet diesen. In Szenarien, in denen der SIP-Provider im „200 OK" nach dem REGISTER im Contact Feld einen kleineren ‚Expires'-Wert vorgab, wurde dieser vom Voice Call Manager nicht berücksichtigt. Dies führte dazu, dass die Registrierung nach Ablauf des ‚Expires'-Wertes abbrach.

LCOS-Änderungen 10.50.0434 RU3

Neue Features

- Der Status der IPv6-Firewall wird nun im WEBconfig-Dashboard angezeigt.
- Bei Logins bzw. Login-Versuchen auf das Gerät wird nun auch die MAC-Adresse (falls verfügbar) der zugreifenden Station protokolliert.
- Mit LCOS 10.50 RU3 wird eine aktualisierte Modem-Firmware für die DSL-Modems der LANCOM 1926-Serie bereitgestellt, welche Stabilitätsverbesserungen für G-FAST und VDSL-Verbindungen enthält.

Korrekturen / Anpassungen

Allgemein

- In der Kommandozeile war beim Befehl ‚ls' eine Filtermöglichkeit per @-Zeichen nicht mehr möglich (z.B. ls Status/Voice-Call-Manager/Lines/ @ „WIZ_T-123456").
- Wenn beim Login auf ein LANCOM Gerät mit dem Benutzerkonto des Root-Administrators kein Benutzername angegeben war, wurde im Event-Log des Gerätes auch kein Benutzername in den jeweiligen Log-Eintrag geschrieben.
- Wenn als Antwort auf einen gesendeten TXT-Record ein leerer TXT-Record empfangen wurde, konnte der DNS-Server im LANCOM Router diese Antwort nicht verarbeiten. In der Folge verwarf dieser die Antwort.
- Ein Zugriff per LL2M auf ein Gerät im Werkszustand ohne gesetztes Passwort war nicht möglich. In diesem Fall wurde die Fehlermeldung „user unknown on remote system" ausgegeben.
- Es konnte beim Versenden einer E-Mail durch den Router zu einem unvermittelten Neustart kommen.
- Bei der Nutzung von OSCP wurde ein abgelaufenes Zertifikat weiterhin verwendet, auch wenn dieses bereits per SCEP erneuert wurde.
- Wenn ein Client eine NAPTR-Anfrage an den Router stellte, kam es mit LCOS 10.50 und aktivierter DNS-Protokollierung im Syslog-Server zu einem unvermittelten Neustart des Routers.

VPN

- Wenn in der Tabelle für weitere entfernte VPN-Gateways ein Eintrag mit einem Routing-Tag angegeben war, für welches es keine Route in der IP-Routing-Tabelle gab, wurde eine VPN-Verbindung bei Nichterreichbarkeit des primären entfernten Gateways auch dann nicht aufgebaut, wenn in der Tabelle ‚Weitere entfernte Gateways' Einträge mit einem Routing-Tag vorhanden waren, für das eine Route existierte.

WLAN

- Per WEBconfig konnte in der LEPS-Konfiguration kein WLAN-Client ohne Angabe einer Passphrase hinzugefügt werden, obwohl die Angabe einer Passphrase optional angegeben war.
- Bei Verwendung der LAN-Bridge auf einem Access Point oder WLAN-Router (Standard-Einstellung) wurde bei DHCP-Requests immer die MAC-Adresse des LAN-Interfaces eingesetzt. Dies führte dazu, dass per WLAN Punkt-zu-Punkt-Verbindung oder per AutoWDS angebundene Access Points oder WLAN-Router das DHCP-Offer verwarfen und somit keine IP-Adresse beziehen konnten.
- Wurden auf einem Access Point mit aktiver DSLoL-Verbindung größere Datenmengen übertragen (etwa durch einen Download oder einen längeren Speedtest), konnte dies zu einem unvermittelten Neustart des Access Points führen.

VoIP

- Wurde in einem Szenario mit einer SIP-TK-Anlage ein Telefonat zwischen zwei Teilnehmern (A und B) mittels der Funktion ‚Halten' an einen dritten Teilnehmer (C) weitergeleitet, beantwortete der LANCOM Router das INVITE (ohne SDP) der TK-Anlage selbst, statt dieses weiterzuleiten. Dies führte dazu, dass anschließend keine RTP-Daten übertragen wurden und somit keine Sprachübertragung zwischen den Teilnehmern A und C möglich war.
- Bei ausgehenden Anrufen an ein Fax-Endgerät konnte es wegen einer „403 Error Response" auf das Re-INVITE mit dem Text „Forbidden - PBX Validation Failed" sporadisch zu einem unvermittelten Neustart des LANCOM Routers kommen, wenn auf dem LANCOM Router die Overlap-Dialing-Funktionalität verwendet wurde.
- Bei der Verwendung von CTI+ an einer Netphone TK-Anlage konnte es in Verbindung mit dem LANCOM VoIP-Router zu einseitiger Sprachübertragung kommen, da die lokal erzeugten RTP-Header nicht mit den durchgereichten RTP-Headern synchronisiert waren.
- Es konnte beim Versand eines SNMP-Traps mit Informationen zu ISDN-Benutzern zu einem unvermittelten Neustart des Routers kommen.

LCOS-Änderungen 10.50.0331 RU2

Neue Features

- Unterstützung für das Modul LANCOM SFP-GPON-1
- Aktualisierung des DSL-Linecodes der LANCOM 1926er-Serie

Korrekturen / Anpassungen

Allgemein

- Durch eine fehlerhafte Sortierung der „Port-Forwarding-Tabelle“ konnte es bei sich überlappenden Einträgen (mit unterschiedlichen Protokollen) vorkommen, dass das Port-Forwarding nicht korrekt funktionierte.
- In einem VRRP-Szenario mit einzelnen WAN-Gegenstellen, in welchem diese Gegenstellen zusätzlich zu einem Loadbalancer zusammengefasst wurden, konnte es vorkommen, dass der VRRP-Slave im Sekundentakt versuchte die WAN-Gegenstellen aufzubauen.
  In der Folge stieg die CPU-Last des Gerätes und es trat ein Speichermangel auf. Es wurde nun eine Pause zwischen den einzelnen Verbindungsversuchen programmiert, wodurch das Gerät nicht mehr an seine Leistungsgrenze gebracht wird.
- Beim LANCOM 1790VA-4G+ wurden Informationen zum verwendeten Mobilfunk-Band nicht im Status angezeigt.
- Bei den LANCOM Routern der 1926er-Serie konnte es zu regelmäßigen Abbrüchen der ADSL- und/oder VDSL-Internetverbindung kommen. Die Internetverbindungen wurden nach einem Abbruch auch nicht automatisch wieder aufgebaut (Neustart behob das Problem bis um nächsten Abbruch).
- Bei aktivierter TR-069-Funktionalität konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.
- Aufgrund eines eingeschränkten Zeichenumfangs konnten bei BGP keine IPv6-Link Local-Adressen verwendet werden.
- Wenn in der Konfiguration eines LANCOM Routers ein IPv4-Adress Pool hinterlegt war und über den Setup-Assistent im WEBconfig eine neue VPN-Einwahl erstellt wurde, konnte der bereits vorhandene Adress-Pool im Setup-Assistent nicht ausgewählt werden.

WLAN

- Es konnte vorkommen, dass im WEBconfig-Menü „**Public Spot Benuter verwalten**“ keine Ausdrucke von angelegten Public-Spot-Benutzerdaten erstellt werden konnten.

VoIP

- In einem Szenario, in welchem eine Panasonic SIP-TK-Anlage (SIP-TK KX-NCP500) an einem LANCOM Router angeschlossen war, konnte eine Anrufweiterleitung aufgrund einer fehlerhaften SDP-Kommunikation seitens der TK-Anlage scheitern. Im LCOS wurde nun ein Workaround eingebaut, welcher den Fehler abfängt und eine Kommunikation ermöglicht.
- Wenn ein ausgehender Anruf vom angerufenen Teilnehmer an einen dritten Teilnehmer weitergeleitet wurde und der dritte Teilnehmer ein DTMF-Menü zur Anrufbearbeitung anbot, funktionierte die DTMF-Kommunikation über Tastentöne nicht mehr. In der Folge konnte das vom dritten Teilnehmer angebotene DTMF-Menü nicht bedient werden.

LCOS-Änderungen 10.50.0235 RU1

Neue Features

- Der Aktivitätsstatus des DNS-Forwarders wird nun auch im WEBconfig-Dashboard unter ‚Dienste' angezeigt.
- **VoIP:** Für TCP-basierte SIP-Leitungen wird nun alle 60 Sekunden ein TCP-Keepalive-Paket gesendet. Das Intervall ist auf der CLI konfigurierbar.

Korrekturen / Anpassungen

Allgemein

- Wenn in der Tabelle der Zugriffsstationen ein Wert eingetragen war, konnte aus der LANCOM Management Cloud (LMC) heraus keine WEBconfig-Session zu einem Gerät aufgebaut werden.
- Beim Abspeichern einer Skript-Konfigurationsdatei in WEBconfig wurde der Datei eine ungültige Dateiendung zugewiesen.
- Bei Eingabe des Befehls ‚show ip-addresses' blieb der Wert für die DHCP-Lease-Time, wenn er den Wert 0 erreicht hatte, auf diesem Wert stehen.
- Ein externes Modem, welches an einem LANCOM Router angeschlossen war und eine sog. APIPA-Adresse (Automatic Private IP Addressing) besaß, konnte vom LANCOM Router nicht erreicht werden, da diese Adressen beim Proxy ARP aus dem LAN nicht zugelassen waren.
- In privaten LMC-Installationen funktionierte der WEBconfig-Fernzugriff über den Webbrowser nicht, wenn zu viele HTTP-Cookies verwendet wurden.
- Bei Verwendung bestimmter DSLAMs auf der Provider-Seite konnte es mit einem LANCOM 1926VAG aufgrund einer Inkompatibilität zwischen dem verbauten DSL-Modem und dem DSLAM vorkommen, dass der DSLAM nicht alle erforderlichen Parameter an das DSL-Modem übermittelte. Dies führte dazu, dass kein DSL-Sync zustande kam und somit auch keine DSL-Verbindung aufgebaut werden konnte.
- Wenn ein LANCOM Router als DNS-Server betrieben wurde, antwortete das Gerät bei SOA- und NS-Anfragen in einigen Fällen mit der Trace-Meldung „bad coded request". In der Folge konnte die Anfrage nicht ausgeführt werden.
- Im WEBconfig (z.B. im Menü ‚Konfiguration / IP-Router / Routing / IPv6-Routing-Tabelle) wurde ein IPv6-Präfix aufgrund einer fehlerhaften HTML-Kodierung falsch dargestellt.
- Erfolgreiche Admin-Logins ins WEBconfig wurden zwar in der Login-Tabelle erfasst, der Zähler für die Logins blieb jedoch unverändert.
- Bei Verwendung einer Loopback-Adresse für den E-Mail-Versand per SMTP wurde die Loopback-Adresse nicht berücksichtigt. Wurde in der Loopback-Adresse ein Routing-Tag abweichend von 0 angegeben, fand für dieses keine Übergabe an den SMTP-Dienst statt und es wurde das Routing-Tag 0 verwendet. Dies konnte dazu führen, dass der E-Mail-Versand nicht möglich war.
- Aufgrund einer Limitierung in der Anzahl der angemeldeten MAC-Adressen konnte die VRRP-Funktion nur auf den ersten 6 ARF-Kontexten verwendet werden. Dies betraf nur Router mit DPAA (19xx-Serie, ISG-1000, ISG-4000 und WLC-1000.

- In einer BGP-Community konnte der Wert 0 nicht verwendet werden.
- Wenn ein Portforwarding mit einem Port zwischen 16384 und 65535 eingerichtet wurde, konnte es vorkommen, dass dieser Port auch für eine dynamische Port-Aushandlung eines weiteren Netzwerk-Teilnehmers verwendet wurde. In diesem Fall wurden die eingehenden Pakete an das Ziel der dynamischen Port-Aushandlung statt an das eigentliche Ziel weitergeleitet.
- Wurde eine Firewall-Regel mit ‚bedingter Übertragung' durchlaufen und es traf keine Bedingung in einer weiteren Firewall-Regel zu, wurde das Paket im IP-Router mit der Fehlermeldung „Network unreachable (no route) => Discard" verworfen, statt das Paket nachträglich per ‚ACCEPT' zu erlauben.
- Der Abgleich der IP-Adresse mit einem DynDNS-Dienst funktionierte bei Verwendung von HTTPS nicht, da der Datenverkehr aufgrund einer zu hohen MTU nicht übertragen werden konnte.
- Pakete aus einem Netzwerk mit zugeordneter LACP-Schnittstelle wurden durch die Firewall verworfen, da die Intruder Detection ein falsches Interface erkannte. In der Folge war die Kommunikation mit diesem Netzwerk nicht möglich.
- Wenn in der Backup-Tabelle eine Backup-Verbindung angegeben wurde, deren Namensbezeichnung kürzer war, als die der Haupt-Verbindung, konnte eine Firewall-Regel, welche ein Stations-Objekt mit der Namensbezeichnung der Haupt-Verbindung enthielt, nicht in das Gerät geschrieben werden.
- Es konnte bei Verwendung von LACP sporadisch vorkommen, dass die Antwort auf ein eingehendes Paket über eine andere LACP-Schnittstelle gesendet wurde. Dies führte dazu, dass das Paket verworfen wurde.
  Auf Routern mit Hardware-Switch (17xx- und 19xx-Serie) wurde in diesem Fall im Ethernet-Trace die Fehlermeldung „sEthSwitchDrvrDscr: WARNING: physical port x is not part of function LAN-x (port mask 0x04), packet will be discarded" ausgegeben. Auf Routern ohne Hardware-Switch (ISG-x000, vRouter) wurden die Pakete stillschweigend verworfen.

WLAN

- Access Points mit einer alten Firmware (z.B. Version 9.24) konnten aufgrund einer fehlerhaften TLS-Aushandlung nicht von einem WLAN-Controller verwaltet werden.
- Es konnte in einem WLC-Cluster-Szenario vorkommen, dass die Sub-CA auf dem Slave ablief und kein neues Zertifikat bezogen wurde. Dies führte dazu, dass die auf dem Slave angemeldeten Access Points nicht verwaltet werden konnten.
- Nach einem Firmware-Update auf LCOS 10.50 konnte es bei einem OAP-830 ohne aktive VPN-Option in Einzelfällen zu einer Bootschleife kommen.
- Wenn bei gesetzter WLAN-Trace-MAC-Adresse ein WLAN-Strength-Trace ausgeführt wurde, kam es zu einem unvermitteltem Neustart des Gerätes.

VoIP

- Bei Szenarien, in welchen ein Swyx-Server mit einer Software kleiner als Version 12.30 verwendet wurde, konnte die Fax-Übertragung vom LANCOM Router zu Swyx aufgrund einer fehlerhaften Transaction-ID fehlschlagen.
- Da vom LANCOM Voice Call Manager gesendete TCP-Keepalive-Pakete ein SYN-Flag enthielten, konnte es vorkommen, dass VoIP-Leitungen, bei denen keine Signalisierungs-Verschlüsselung verwendet wurde, die Registrierung verloren.

LCOS-Änderungen 10.50.0145 Rel

Neue Features

- Unterstützung von RADIUS Dynamic Peer Discovery nach RFC 7585

Korrekturen / Anpassungen

Allgemein

- Beim Anlegen eines RADIUS-Benutzers über WEBconfig konnte das Benutzerprofil nicht gespeichert werden, wenn dort keine Passphrase eingetragen wurde.
- Mit dem Konsolenbefehl ‚passwd -n' kann eine Passwortänderung ohne Abfrage durchgeführt werden. Dabei wurde die Änderung nicht für den SNMP-Zugriff übernommen, sodass ein SNMP-Zugriff mit dem alten Passwort möglich war. (CVE-2021-33903)
- Bei Verwendung von Zertifikaten mit ‚Elliptic Curve Algorithmus' für RADSEC konnte die TLS-Aushandlung nicht erfolgreich abgeschlossen werden.
  Weiterhin konnte der ‚Private Key' eines Zertifikats mit ‚Elliptic Curve Algorithmus' nicht in den RADSEC-Slot hochgeladen werden. Der Import-Vorgang wurde mit der Meldung „FAILURE" abgebrochen.

VPN

- Versuchte der Router während eines VPN-Aufbaus im Zeitfenster zwischen IKE-Aushandlung und dem Wechsel in den Status ‚Up' ein Paket über die VPN-Verbindung zu senden, wurden alle Pakete verworfen.
- Nach einem Abbau und anschließendem Neu-Aufbau einer VPN-Verbindung (sowohl IKEv1 als auch IKEv2) mit IPv6 auf einem vRouter oder LANCOM ISG-8000 wurden die VPN-Regeln (SA) nicht korrekt aufgebaut. Dadurch war keine Kommunikation über die VPN-Verbindung mehr möglich.

VoIP

- Es konnte vorkommen, dass Telefonate über den SIP-ALG nicht übertragen wurden, da der externe Port vom Router als ungültig deklariert wurde. Die Pakete wurden dann mit der Fehlermeldung „ICMP Destination unreachable (Port unreachable)" abgelehnt.
  Weiterhin funktionierte die Bandbreiten-Reservierung im SIP-ALG nicht mehr.
- In einem Szenario mit einer Swyx Mediabridge erfolgt nach Rufaufbau ein REFER mit dem eigentlichen Ziel des Telefonates im ‚Refer-To'-Header. Daraufhin sendet der Router ein INVITE zu diesem ‚Refer-To'-Ziel über die Swyx TK-Anlage. Im Fehlerfall antwortete die Swyx TK-Anlage nicht mit einem „200 OK" sondern mit der Fehlermeldung „500 Server Internal Error". Der Router versuchte in diesem Fall das INVITE auf einer anderen Leitung zu senden. Da hierfür aber noch die Replace-Informationen aus dem REFER verwendet wurden, sendete der Router das INVITE erneut über die Gateway-Leitung an die Swyx TK-Anlage.

Ein INVITE wird jetzt nicht mehr auf einer Gateway-Leitung versendet, nachdem auf dieser die Fehlermeldung „500 Server Internal Error“ empfangen wurde. Weiterhin wartet der Router auf ein BYE der Swyx TK-Anlage und beendet anschließend den Rufaufbau. Wenn kein BYE von der Swyx TK-Anlage empfangen wird, sendet der Router das BYE und beendet den Rufaufbau.

- In Einzelfällen kann es vorkommen, dass bei einem eingehenden Telefonat während der Early-Media-Phase ein UPDATE vom Anrufer anstatt vom Angerufenen gesendet wird. In einem solchen Fall wurde das UPDATE vom Router wieder auf die SIP-Leitung gesendet statt an den lokalen Teilnehmer. Dies führte zu einer einseitigen Sprachübertragung.
- Werden in einem Szenario mit einer übergeordneten SIP-TK-Anlage bei einem ausgehenden Telefonat in den Sitzungen zwischen Router und SIP-Client sowie Router und SIP-TK-Anlage unterschiedliche Codecs verwendet, so muss der Codec mit dem SIP-Client in einem Re-INVITE neu ausgehandelt werden, sodass der Codec übereinstimmt. Wenn die SIP-TK-Anlage in diesem Moment ein Re-INVITE zur Weiterleitung des Telefonats an den Router sendete, wurde dieses vom Router an den SIP-Client gesendet, obwohl das erste Re-INVITE noch nicht bestätigt wurde. Dies führte zu fehlender Sprachübertragung in Verbindung mit einem Rauschen bei dem anrufenden Teilnehmer.

  Die Übermittlung des zweiten Re-INVITEs der SIP-TK-Anlage wird jetzt erst übertragen, wenn die erste Aushandlung abgeschlossen ist.

LCOS-Änderungen 10.50.0129 RC3

Neue Features

Allgemein

- Neuer DSL-Linecode für Geräte der LANCOM 1926-Serie
- Auf den DSL-Routern der Serien 19xx und 179x kann zwischen dem aktuellem und einem alternativem DSL-Linecode umgeschaltet werden.
- Unterstützung eines DNS-Filters zur Erkennung und Filterung von ungewünschten DNS-Datentunneln auf der Clientseite.
- Unterstützung von IPv6 Prefix Discovery bei 464XLAT nach RFC 7050
- Der WLC schaltet DNS-Server und DNS-Forwarder auf verwalteten APs ab.
- Neuer VPN-Analyse-Befehl ‚ikectl' auf der Kommandozeile
- Unterstützung von automatischer Path MTU Detection bei IPSec.

Korrekturen / Anpassungen

Allgemein

- Im WEBconfig konnten nur die Benutzerdaten eines ausgewählten Public Spot-Benutzers ausgedruckt werden. Wenn mehrere Benutzerdatensätze zum Druck ausgewählt wurden, endete der Druckvorgang in einer endlosen Ladeschleife.
- Ein Zugriff per LL2M auf ein Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „user unknown on remote system" quittiert.
- Das Erstellen eines Wireshark-Trace per LCOSCap auf einem Gerät mit gehashtem Passwort schlug fehl und wurde mit der Fehlermeldung „cannot retrieve PSK" quittiert.

LCOS-Änderungen 10.50.0115 RC2

Neue Features

WLAN

- Unterstützung für Fast Roaming over-the-DS

Korrekturen / Anpassungen

Allgemein

- Nach einer Aktualisierung auf LCOS 10.50 RC1 konnte es vorkommen, dass nach einer Konfigurations-Synchronisierung mit der LANCOM Management Cloud (LMC) eine Firewall-Regel, welche ein DNS-Ziel enthielt, nicht mehr mit LANconfig editiert werden konnte.
- Es konnte in Einzelfällen vorkommen, dass Sessions nicht ordnungsgemäß abgebaut wurden (u.a. bei Verwendung von IPSec-over-HTTPS) und der reservierte Speicher nicht wieder freigegeben wurde. Dies führte dazu, dass weitere Pakete verworfen wurden und die Kommunikation nur noch stark eingeschränkt möglich war.
- Bei Verwendung des Stationsobjektes LOCALNET in Firewall-Regeln wurden per RIP und BGP gelernte Routen dem LOCALNET zugeordnet. Dies konnte dazu führen, dass die CPU des Routers aufgrund sehr vieler Filter-Regeln eine hohe Auslastung aufwies.
  Dem Stationsobjekt LOCALNET werden jetzt nur noch Netzwerke im Status ‚Connected LAN' zugeordnet.

LCOS-Änderungen 10.50.0091 RC1

Neue Features

- Performance-Optimierung durch Multicore-Unterstützung für LANCOM ISG-8000 bei IPsec-VPN
- Unterstützung von Bidirectional Forwarding Detection (BFD) bei BGP
- (Sub-Second-)Session-Switchover für Dynamic Path Selection (DPS)
- DPS: ICMP-Messintervalle unterstützen nun Intervalle mit einer Zeitauflösung in Millisekunden
- DPS: Neben ICMP wird auch HTTP(S) als Messmethode unterstützt
- Unterstützung der CLAT-Seite von 464XLAT für IPv6-only im Mobilfunk
- Unterstützung von NPTv6 (Präfix-NAT) bei IPv6
- Der Loadbalancer unterstützt nun IPv6.
- Unterstützung von IPv6-Leitungs-Polling
- In der IPv6-Firewall können MAC-Adressen als Stationsobjekt (Quelle) konfiguriert werden.
- In der IPv6-Firewall kann ein delegiertes Provider-Präfix als Stationsobjekt konfiguriert werden um ein dynamisches Präfix in einer Router-Kaskade freizugeben.

- In Anwendungen, in denen DNS-Namen konfiguriert werden können, kann die bevorzugte Adressfamilie (IPv4 oder IPv6) angegeben werden.
- Dynamic Path Selection (DPS) unterstützt nun IPv6.
- Unterstützung für Curve448 im SSH
- Der Public Spot unterstützt nun IPv6.
- Public Spot: Das MAC-Adressformat ist nun konfigurierbar.
- Unterstützung für RADIUS-Attribute nach RFC 5580
- Der DHCP-Client zeigt nun die Lease-Time im Status-Menü an.
- Die Rx / Tx Bandbreitenbegrenzung wird nun auch bei bei 802.1x-RADIUS-Authentifzierung ausgewertet.
- Die Layer-7-Anwendungserkennung und DNS-Namen in der Firewall sind nun in einer gemeinsamen Tabelle zu konfigurieren.
- Support von Session-Cookie und Anti-CSRF-Token in der WEBconfig.
- Klartextpasswörter des Hauptgerätepasswords sind nach einem Gerätereset deaktiviert.
- Die IKEv2-Lifetimes sind nach einem Gerätereset an die aktuellen BSI-Empfehlungen angepasst.
- SHA-1 ist nach einem Gerätereset nicht mehr im IKEv2-Default-Proposal enthalten.
- Das delegierte IPv6-Provider Präfix kann über IKEv2-Routing an die VPN-Gegenstelle übermittelt werden.
- Die Unterstützung für H.323 in der IPv4-Firewall entfällt.
- Der vRouter unterstützt nun KVM als Hypervisor-Plattform.

Korrekturen / Anpassungen

VoIP

- Sendete ein VoIP-Client bei einem ausgehenden Anruf den Parameter ‚rtcp-rsize' mit, erkannte der LANCOM Router diesen Parameter als ‚Invalid' und lehnte das ‚Invite' mit der Meldung „406 SDP - not acceptable" ab. In der Folge kam der ausgehende Ruf nicht zustande.
- Bei einem eingehenden ISDN-Anruf konnte es vorkommen, dass der externe Anrufer den Angerufenen nicht hören konnte (einseitige Sprachübertragung), da das ‚Media Attribute (a): nortpproxy:yes' die Übermittlung von RTP-Daten verhinderte.
- Bei Verwendung des SIP-ALG konnte es vorkommen, dass der Port für die RTP-Kommunikation ungültig wurde und ein eingehendes RTP-Paket mit der Meldung „ICMP Destination unreachable (Port unreachable)" abgelehnt wurde. Dies führte bei einem ausgehenden Telefonat zu einer einseitigen Sprachübertragung seitens des angerufenen Teilnehmers.
- Der Voice Call Manager unterstützt mehrere Streams mit verschiedenen Codecs. Diese müssen aber während des Rufaufbaus initialisiert werden.
  Wurde ein Anruf initial mit einem Stream aufgebaut (z.B. G.711) und im Re-INVITE ein zweiter Stream hinzugefügt (z.B. T.38), konnte der Voice Call Manager den zweiten Stream nicht verarbeiten. Dadurch wurden Daten-Pakete des zweiten Streams nicht weiter übertragen.

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.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. 02/22