Release Notes

LCOS
10.90 RC2

Inhaltsübersicht

03 **1. Einleitung**

03 **2. Das Release-Tag in der Software-Bezeichnung**

04 **3. Gerätespezifische Kompatibilität zu LCOS 10.90**
04 LANCOM Geräte ohne Unterstützung ab LCOS 10.90

04 **4. Hinweise zu LCOS 10.90**
04 Allgemeine Hinweise zum Update
05 Informationen zu Werkseinstellungen

06 **5. Feature-Übersicht LCOS 10.90**

06 **5.1 Feature-Highlights**
06 Sicherstellung geschäftskritischer Anwendungen dank Unterstützung von acht QoS-Queues
06 MOBIKE im VPN für einen beschleunigten Netzwerkwechsel
06 Höchste Ausfallsicherheit mit VRRPv3 für Dual-Stack-Netzwerke

07 **5.2 Weitere Features**

08 **6. Historie LCOS 10.90**
08 LCOS-Änderungen 10.90.0076 RC2
10 LCOS-Änderungen 10.90.0059 RC1

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

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 10.90 RC2 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Updates unbedingt die Hinweise im Kapitel 7 „Allgemeine Hinweise“ dieses Dokumentes.

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

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS 10.90

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

LANCOM Geräte ohne Unterstützung ab LCOS 10.90

→ LANCOM R800V
→ LANCOM LN-630acn
→ LANCOM 1781VA
→ LANCOM 1906VA-4G
→ LANCOM L-322agn (R2)
→ LANCOM LN-862
→ LANCOM LN-860
→ LANCOM OAP-830
→ LANCOM OAP-1700B
→ LANCOM OAP-821
→ LANCOM OAP-822
→ LANCOM IAP-1781VAW(+)

4. Hinweise zu LCOS 10.90

Allgemeine Hinweise zum Update

Ab LCOS 10.90 wurde das CLI-Menü für VRRP von ‚/Setup/IP-Router/VRRP/' nach ‚/Setup/VRRP/' verschoben. Die Tabellenstruktur sowie der zugehörige OID-Pfad hat sich aufgrund der Unterstützung für VRRPv3 und IPv6 ebenfalls geändert.
Bitte beachten Sie, dass Add-Ins für die LMC sowie ggf. vorhande Scripte für VRRP für LCOS 10.90 und höher angepasst werden müssen. Existierende Scripte für VRRP sind nicht mit LCOS 10.90 und höher kompatibel.

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.

5. Feature-Übersicht LCOS 10.90

5.1 Feature-Highlights

Sicherstellung geschäftskritischer Anwendungen dank Unterstützung von acht QoS-Queues

Dieses Feature ermöglicht es Ihnen, bis zu acht verschiedene Queues (Serviceklassen) mit entsprechenden Prioritätsstufen für Anwendungen im Netzwerk festzulegen (z. B. „VoIP“, „Gold“, „Silber“ oder „Best Effort“). Ihre Datenpakete werden mithilfe von DSCP-Markierungen oder durch Firewallregeln der entsprechenden Quality of Service (QoS)-Klasse zugeordnet. Das Gateway sortiert anschließend die Pakete in die richtige Prioritätsstufe und stellt sicher, dass die entsprechenden Dienste nur so viel Upload-Bandbreite nutzen, wie für ihre Klasse zuvor von Ihnen in Prozent oder MBit/s konfiguriert wurde. Auf diese Weise wird sichergestellt, dass wichtige Dienste wie VoIP oder Videoanrufe stets ausreichend Bandbreite erhalten, selbst bei hoher Netzwerkauslastung.

MOBIKE im VPN für einen beschleunigten Netzwerkwechsel

Mit der MOBIKE-Erweiterung für IKEv2 können VPN-Clients nahtlos zwischen verschiedenen Netzwerken wechseln (z. B. von WLAN zu Mobilfunk), ohne den VPN-Tunnel neu aufbauen zu müssen. Der LANCOM Advanced VPN Client oder LANCOM Trusted Access Client sendet beim Netzwechsel eine Aktualisierungsnachricht mit seiner neuen IP-Adresse an das SD-WAN-Gateway. Für Sie bedeutet das: Keine Unterbrechung beim VPN-Roaming, die Verbindung bleibt stabil.

Höchste Ausfallsicherheit mit VRRPv3 für Dual-Stack-Netzwerke

VRRPv3 für IPv6 ermöglicht es Ihnen, Router-Redundanz auch in Netzwerken mit IPv6 oder in Dual-Stack-Umgebungen (gleichzeitige Nutzung von IPv4 und IPv6) zu implementieren. Dies erhöht die Betriebssicherheit, da bei einem Ausfall eines Routers ein anderer automatisch die Funktion übernehmen kann. Diese Funktion ist ideal für moderne Netzwerke, die sowohl IPv4 als auch IPv6 unterstützen, da sie eine nahtlose Redundanz in beiden Protokollen gewährleistet.

5.2 Weitere Features

→ Dank Post-Quantum Preshared Keys bei IKEv2 können VPNs bereits heute gegen potenzielle zukünftige Angriffe von Quantencomputern abgesichert werden. Diese Technologie fügt zusätzliche Sicherheitsmechanismen hinzu, um die Verschlüsselung langfristig zu schützen – selbst wenn Quantencomputer in der Lage sein sollten, traditionelle Verschlüsselungsmethoden zu brechen. .

→ Mit LCOS 10.90 RC1 kann der Router im LAN dynamisch VLANs per RADIUS an IEEE 802.1X-Clients zuweisen. Eine aufwendige physische Infrastruktur, wie dedizierte Switches, wird nicht benötigt, um eine VLAN-Trennung und -Zuordnung durchzuführen. Da der Router die gesamte LAN-Sicherheitsstruktur übernimmt, ist dieses Feature ideal für kleine Standorte.

→ Viele weitere Verbesserungen für die Administration und den Betrieb moderner Netzwerke

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 6 „Historie LCOS“.

6. Historie LCOS 10.90

LCOS-Änderungen 10.90.0076 RC2

Neue Features

→ Unterstützung für IKEv2 EAP-OTP 2FA für den LANCOM Advanced VPN Client macOS

→ Der TCP/HTTP-Tunnel kann nun auch per CLI-Kommando erzeugt werden.

→ **VoIP:** Der Voice Call Manager markiert IPv6 RTP-Pakete nun so, dass diese auch in die Urgent Queue des neuen QoS gesendet werden.

→ Die maximale Anzahl für Public Key-Authentifizierungsversuche im SSH ist jetzt konfigurierbar.

→ **VRRP:** Es ist nun konfigurierbar, dass eine WAN-Verbindung überwacht, aber im Standby-Fall der Aufbau der WAN-Verbindung nicht unterdrückt werden soll.

Korrekturen / Anpassungen

Allgemein

→ Wenn in der Kommandozeile der Befehl „find vrrp“ eingegeben wurde, enthielten die ausgegebenen Pfad-Informationen keine Zeilenumbrüche.

→ Waren bei einer VPN-Loadbalancer-Konfiguration als IPv4/IPv6-Zieladressen DNS-Adressen statt IP-Adressen angegeben, füllte sich die Tabelle im Pfad ‚Status/VPN/Load-Balancer/Peer-Status/‘ mit unendlich vielen Einträgen.

→ Bei einigen LANCOM Geräten, die mit der LMC verbunden waren, konnte es zu einem Stack Overlow im HTTP-Client kommen, was dazu führte, dass die Geräte unvermittelt neu starteten.

→ In einem VRRP-Szenario mit VPN Load Balancer (VLB), in welchem IPv6-Adressen verwendet wurden, kam es nach einem Neustart zu einem Timing-Problem zwischen dem Start des IPv6-VRRPv3 und dem VLB. In der Folge startete der VLB nicht mehr eigenständig und musste manuell gestartet werden.

→ Eine Plain-Ethernet-Gegenstelle mit dynamisch erzeugter MAC-Adresse (‚MAC-Adress-Typ‘ auf ‚Lokal‘) eines in Hyper-V betriebenen vRouters wurde nicht aufgebaut, sodass die Internet-Verbindung nicht zustande kam. Weiterhin konnten in einem solchen Szenario mehrere im vRouter angelegte Plain-Ethernet-Gegenstellen mit dynamischer MAC-Adresse untereinander keine ICMP-Pakete (Ping) austauschen.

→ Bei Mobilfunk-Routern mit Quectel 4G- und 5G-Modulen wurde die Provider-Bezeichnung im Status-Feld ‚Network' (Konsolen-Pfad ‚Status/Modem-Mobile/') auf 16 Zeichen begrenzt. Dadurch konnte es vorkommen, dass die Bezeichnung abgeschnitten wurde.
Die folgenden LANCOM Mobilfunk-Router waren von dem Verhalten betroffen:
- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

VoIP

→ Aktive Telefonate wurden nach Deaktivierung des Voice Call Managers nicht abgebaut und blieben weiterhin aktiv.

LCOS-Änderungen 10.90.0059 RC1

Neue Features

Allgemein:

→ Erweiterungen im QoS: Unterstützung von 8 QoS-Queues für IPv4 und IPv6.
→ Unterstützung von VRRPv3 für IPv4 und IPv6
→ Unterstützung von dynamischer VLAN-Zuweisung auf dem LAN bei 802.1X per RADIUS
→ Unterstützung AES-CMAC im NTP nach RFC 8573
→ Unterstützung im Syslog-Client zur Formatierung der Nachrichten nach RFC 5424
→ Unterstützung von TLS im Syslog-Client
→ Unterstützung von MTU 1500 im PPPoE nach RFC 4638
→ In der Ethernetport-Tabelle wurde ein Kommentarfeld hinzugefügt.
→ Unterstützung für stabile IPv6 Privacy Interface Identifier nach RFC 7217
→ Unterstützung für RFC 8268 im SSH um zusätzlich DH-Gruppen
→ Das TR-069-Datenmodell ist im Default nun TR-181.
→ Die xDSL-Verbindungshistorie ist nun bootpersistent.
→ Unterstützung des IPerf-Reverse-Mode-Parameters
→ Die Passwortrichtlinie für das Hauptgerätepasswort ist nur granularer konfigurierbar.
→ Der VDSL-/ADSL-Linecode wurde aktualisiert.
→ Es können nun auch Skripte importiert und exportiert werden, die nur die Verschlüsselung von Passwörtern mit einem benutzerdefinierten Passwort beinhalten.
→ Der Alive-Test wurde um einen benutzerdefinierten Befehl erweitert, der beim Übergang vom Fehlerfall zurück zum normalen Zustand einmalig ausgeführt werden kann.
→ Unterstützung der Captive Portal API nach RFC 8908 und RFC 8910 im Public Spot
→ Der IAP-5G unterstützt nun auch TR-069.
→ Der DNS-Forwarder unterstützt nun auch administrative Distanzen. Ändert sich die Default-Route aufgrund von administrativen Distanzen, so verwendet der DNS-Forwarder nun die neue bessere Route.
→ Unterstützung von IEEE 802.1ag OAM-Funktionen
→ Unterstützung für Ethernet Link-OAM 802.3ah Remote Loopback Mode
→ Unterstützung des WWAN-Firmware-Updates beim 1800EF-4G

→ Das Reboot-Kommando auf der CLI unterstützt nun die Option zur zeitgesteuerten, einmaligen Ausführung des Reboots.
→ Das 1TR-112 Prioritätstagging für VLANs auf der WAN-Verbindung wurde auf den aktuellen gültigen Standard angepasst.
→ Erweiterungen im IPerf um zusätzliche CLI-Parameter
→ Das Ping-Kommando unterstützt nun den Tracepath-Modus zur Ermittlung der MTU des Ping-Ziels (Option -m).
→ Wird ein logischer DSL-Kanal zwei oder mehr physischen Ethernet-Ports zugeordnet, wird nur noch der erste (aktive) Ethernet-Port verwendet. Es ist nicht mehr möglich, zwei oder mehr unterschiedliche aktive ETH-Ports gleichzeitig mit einem logischen DSL-Kanal zu betreiben.
→ Änderungen bzw. Entfall für Konfigurationsparameter für USB-Autoload: Die Konfigurations- und / oder Skript-Dateien werden nur dann automatisch in das Gerät geladen, wenn sich das Gerät im Auslieferungszustand befindet.

VPN

→ Unterstützung von MOBIKE im IKEv2 als Responder-Rolle
→ Unterstützung von ‚Quantum-Safe Encryption Using Postquantum Preshared Keys' bei IKEv2 nach RFC 8784
→ Die Subnetzmaske bei IPv4 bzw. Präfixlänge bei IPv6 kann IKEv2 Config-Mode-Clients zugewiesen werden.
→ Unterstützung von Null-Encryption im ESP bei IKEv2
→ Die verwendeten DH-Gruppen eines aktiven VPN-Tunnels werden nun im Status unter /Status/VPN/IKE und /Status/VPN/IKE angezeigt.

Entfallene Features

→ Entfall von Cast128-CBC-, Blowfish-CBC- und DES-Verschlüsselungsalgorithmen im IKEv1
→ Entfall des IKEv1 myVPN-Features
→ Entfall von Analog-Modemverbindungen und ISDN-Einwahlen
→ Entfall der ISDN-Standortverifikation
→ Entfall ISDN-Zeitbezug
→ Entfall CLIP bei RAS-Einwahl
→ Entfall ISDN-Gegenstellen-Tabelle (für Wählverbindungen)
→ Entfall X.25 Bridge
→ Entfall AsyncPPP
→ Entfall Multilink-PPP
→ Entfall LANcapi, Fax
→ Entfall CBCP (Callback Control Protocol) im PPP
→ Entfall Dynamic-VPN über D- und B-Kanal

→ Entfall Least Cost Router
→ Entfall der Unterstützung von externen 2G/3G-USB-Modems
→ Entfall der NetBios-Funktionen (Netbios-Proxy, NBNS)

Korrekturen / Anpassungen

Allgemein

→ Wenn eine Internet-Verbindung nicht mehr aufgebaut werden konnte (etwa bei einem Retrain des VDSL-Modems), wurde die Fehlermeldung in WEBconfig doppelt angezeigt.
→ Nachdem bei einem IPv6-Interface mit statisch konfigurierten Delegierungs-Adressen das IPv6-Interface deaktiviert und die Delegierungs-Adressen gelöscht wurden, waren die Delegierungs-Adressen nach Aktivierung des IPv6-Interfaces weiterhin vorhanden.
→ Ein IPv6-Interface soll nur dann nicht aufgebaut werden, wenn die DAD (IPv6 Duplicate Address Detection) bei der primären Link-Local-Adresse nicht erfolgreich ist. Das IPv6-Interface wurde aber auch dann nicht aufgebaut, wenn die DAD bei einer statisch vergebenen IPv6-Adresse, die vor der primären Link-Local-Adresse geprüft wurde, nicht erfolgreich war.
→ Auf Mobilfunk-Routern mit Quectel 4G- und 5G-Modulen wurde bei der Berechnung der Signalwerte RSRP (Reference Signals Received Power) und RSRQ (Reference Signal Received Quality) das Feld für den RSRP übersprungen. Dies führte dazu, dass für den RSRP und den RSRQ fehlerhafte und teils auch physikalisch unmögliche Werte ausgegeben wurden.
Die folgenden Mobilfunk-Router waren von dem Verhalten betroffen:
- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

VPN

→ Auf einem Router mit einer IKEv2-Client-Einwahl mit RADIUS-Authentifizierung per EAP-TLS sendete der Router bei Ablehnung des RADIUS-Servers (z.B. aufgrund von fehlerhaften Login-Daten) das EAP-Failure im letzten vom VPN-Client erhaltenen EAP-Response mit der Notification AUTHENTICATION_FAILED an den VPN-Client.
Der Router sendet das EAP-Failure jetzt im letzten vom VPN-Client erhaltenen IKE_AUTH-Response mit dem EAP Message Code FAILURE.

7. 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 Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de