

LANCOM Release Notes

LCOS 10.20 Rel

Copyright (c) 2002-2018 LANCOM Systems GmbH, Würselen (Germany)

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

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

09.11.2018, CBuersch

Inhaltsübersicht

1. Einleitung	2
2. Gerätespezifische Kompatibilität zu LCOS 10.20	2
3. Hinweise zu LCOS 10.20	3
3.1 Informationen zu Werkseinstellungen	3
3.2 Informationen zum LANCOM vRouter	3
4. Feature-Übersicht LCOS 10.20	4
4.1 Feature-Highlights	4
4.2 Weitere Features	5
5. Historie LCOS 10.20	6
LCOS-Änderungen 10.20.0145 RC2 > 10.20.0175 Rel	6
LCOS-Änderungen 10.20.0097 RC1 > 10.20.0145 RC2	8
LCOS-Änderungen zu 10.20.0097 RC1	10
6. Allgemeine Hinweise	12
Haftungsausschluss	12
Sichern der aktuellen Konfiguration	12
Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes	12

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 Rel sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 6 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite

<https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/>

2. Gerätespezifische Kompatibilität zu LCOS 10.20

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 unterstützte LCOS-Version für Ihr Gerät finden Sie unter

<https://www.lancom-systems.de/produkte/lcos/lifecycle-management/produkttabellen/>

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

3. Hinweise zu LCOS 10.20

3.1 Informationen zu Werkseinstellungen

Geräte, die mit LCOS 10.00 oder größer ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme von neuen Geräten. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

3.2 Informationen zum LANCOM vRouter

Wenn Sie eine vRouter-Instanz erstmalig mit LCOS 10.20 RC1 oder LCOS 10.20 RC2 installiert haben, ist es notwendig, den vRouter mit LCOS 10.20 Rel neu zu installieren. Die generelle Verfügbarkeit des LANCOM vRouter für Microsoft Hyper-V folgt mit einem zukünftigen LCOS Release Update.

4. Feature-Übersicht LCOS 10.20

4.1 Feature-Highlights

WPA3 – WLAN-Sicherheit auf neuestem Stand

Mehr Sicherheit für Ihre WLAN-Infrastruktur bietet Ihnen ab sofort die jüngste Generation der WLAN-Verschlüsselung - WPA3 (Wi-Fi Protected Access). Als Nachfolger von WPA2, bietet WPA3 wichtige Erweiterungen und Sicherheits-Features für kleine („WPA3-Personal“) und große Netze („WPA3-Enterprise“). Mit LCOS 10.20 unterstützen alle LANCOM Access Points und WLAN-Router den neuen WLAN-Sicherheitsstandard. Erfahren Sie mehr in unserem [Whitepaper](#).

Auto Updater – Immer up-to-date

Immer auf dem aktuellen Stand: LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Client Management – Für einfach bestes WLAN

Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dies steigert die Qualität drahtloser Netzwerke - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die bislang getrennten Funktionen Band Steering und Client Steering werden hierbei kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.

LEPS-U & LEPS-MAC – Volle Zugangskontrolle für Ihr WLAN

Bewahren Sie die Kontrolle darüber, wer sich in Ihrem WLAN befindet. Mit LEPS-U (LANCOM Enhanced Passphrase Security-User) vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort für eine SSID. Über LEPS-MAC identifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse - ideal für sichere Unternehmensnetzwerke!

WAN Policy-Based NAT – Nutzung von NAT in Firewall-Regeln

WAN Policy-Based NAT ermöglicht die einfache Zuordnung von statischen WAN-IPv4-Adressen zu gewünschten Diensten. Durch eine NAT-Aktion in den Firewall-Regeln werden dabei interne Adressen hinter einer vom Provider zugewiesenen WAN-Adresse maskiert. Ideal für Szenarien z.B. für den Betrieb von Mailservern und Webservern mit verschiedenen WAN-Adressen.

4.2 Weitere Features

Enhanced Open

Dank Einführung einer zusätzlichen Datenverschlüsselung verbessert Enhanced Open die Sicherheit von Clients in offenen WLANs wie z.B. Hotspots in Cafés oder Hotels.

DSL-Bridge-Mode

Ab sofort können alle VDSL-Router in einen DSL-Bridge-Modus versetzt werden. Dies ermöglicht den Einsatz der Geräte als reines DSL-Modem. Ideal für Szenarien, in denen mehrere DSL-Zugänge an einem Router betrieben werden sollen.

Noch mehr Flexibilität für den LANCOM vRouter

Ab sofort unterstützt der LANCOM vRouter die Virtualisierungsplattform Microsoft Hyper-V. Darüber hinaus wird das Management des vRouters nun noch einfacher, denn Firmware-Updates können fortan einfach via UPX-Datei eingespielt werden.

OCSP-Responder – Neue Power für Smart Certificate

Maximale Sicherheit bei VPN-Zugriffen: Dank Smart Certificate profitieren Sie von der in LANCOM Geräten integrierten Funktion zur komfortablen Erstellung digitaler Zertifikate - ganz ohne externe Zertifizierungsstelle! Erweitert wurde diese Funktion nun um das Netzwerkprotokoll OCSP (Online Certificate Status Protocol), welches Clients ermöglicht, den Status von X.509-Zertifikaten bei der integrierten CA automatisch und effizient abzufragen.

Unterstützung von LISP (Locator/ID Separation Protocol)

Das Locator/ID Separation Protocol (LISP) ist eine neue Routing-Architektur. Mit LISP kann eine hochskalierbare Netzwerke mit integriertem Routing- und Tunnel- bzw. Overlay-Protokoll realisiert werden. Ideal für Service Provider oder Enterprise-Netzwerke.

Public Spot CSV-Import

Public Spot-Management noch einfacher: Benutzer können nun bequem per Textdatei (CSV) für den Hotspot-Zugriff importiert und exportiert werden.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 5 „Historie LCOS 10.20“.

5. Historie LCOS 10.20

LCOS-Änderungen 10.20.0145 RC2 > 10.20.0175 Rel

Neue Features

ab LCOS 10.20 ist der Voice Call Manager (VCM) für folgende Geräte per Default freigeschaltet:

- > LANCOM 1900EF
- > LANCOM ISG-1000
- > LANCOM ISG-4000

Bei folgenden Geräten kann der VCM per All-IP Option freigeschaltet werden:

- > LANCOM 1640E
- > LANCOM 1780EW-4G+
- > LANCOM 1790-4G
- > LANCOM 7100+ VPN
- > LANCOM 9100+ VPN

Korrekturen / Anpassungen

Allgemein

- > Die Routing-Methode „DiffServ-Feld beachten“ funktionierte nicht korrekt, da Pakete, die mit AFxx markiert waren, nicht der Sende-Queue „SAFE“, sondern ebenfalls der Sende-Queue „URGENT“ zugeordnet wurden. Dies führte bei Nutzung von QoS-Regeln dazu, dass diese keinen Effekt hatten, da nicht nur die zu bevorzugenden, sondern auch untergeordnete Pakete über die URGENT-Queue weitergeleitet wurden.
- > In der Service-Tabelle unter Status/Config/Services/ wurde bei aktiviertem SNMP sowohl SNMPv1/2 als auch SNMPv3 als aktiv angezeigt, auch wenn eines der beiden Protokolle nicht aktiv war. Dies wird jetzt für jedes Protokoll getrennt angezeigt.
- > Bei aktiviertem ICMP-Polling wurden Mobilfunk-Verbindungen nach dem Verbindungsaufbau direkt wieder abgebaut, da das Polling fehlschlug.
- > Das Mobilfunkmodul MC7710, welches im LANCOM 1781VA-4G verbaut ist, hat für einige Mobilfunk-Provider fehlerhafte Werte für den Netzwerknamen zurückgemeldet, so dass die gleichen fehlerhaften Werte im LCOS oder im LANmonitor angezeigt wurde. In einem solchen Fall wird nun die numerische Kennung des Provider-Netzwerks angezeigt.

VPN

- › Unter Verwendung von IKEv2 mit aktiviertem PFS konnte es sporadisch nach einem Rekeying oder direkt nach Verbindungsaufbau zu einschlafenden ESP-Tunneln (Tunnel konnte für Datenkommunikation nicht mehr genutzt werden) kommen, wenn der LANCOM Router die VPN-Verbindung zu einem Drittanbieter aufbaute.

WLAN

- › Wenn ein LANCOM Gerät, welches mit der LANCOM Public Spot XL Option kompatibel ist, mit der LANCOM Management Cloud gekoppelt wurde, aktivierte sich die Public Spot XL Option nicht automatisch auf dem Gerät.

VoIP

- › Wurde als SIP-Registrar eine SIP-Domäne hinterlegt, die statt auf die IP-Adresse (CNAME) auf einen weiteren Alias-Namen verwies, so war die SIP-Registrierung nicht möglich.

LCOS-Änderungen 10.20.0097 RC1 > 10.20.0145 RC2

Neue Features

- > LANCOM Auto-Updater für automatische Firmware-Updates
- > Unterstützung von WPA3
- > Enhanced Open für verbesserte Sicherheit von Clients in offenen WLANs
- > Redistribution von RIP-Routen im BGP

Korrekturen / Anpassungen

Allgemein

- > Der DHCP-Adressbezug über WLC- oder EoGRE-Tunnel konnte aufgrund von Verarbeitungsproblemen bei IP-Paketen fehlschlagen. In seltenen Fällen konnte es auch zu einem unvermittelten Neustart des Gerätes kommen.
- > Aufgrund einer falschen Kanaluordnung bei WLAN-Routern wurde eine IPoE-Verbindung, die auf einem DSL-Interface konfiguriert wurde (z.B. DSL-1), einem ISDN-Interface zugeordnet.
- > Bei Verwendung einer Backup-Verbindung über die Backup-Tabelle kam es beim Wechsel von der Haupt- auf die Backup-Verbindung dazu, dass TCP-Sessions nicht auf die Backup-Verbindung übernommen oder nicht korrekt terminiert wurden. Auch wurden DNS-Anfragen nach Aufbau der Backup-Verbindung nicht über diese versendet.
- > Wenn der Zugriff auf das Management-Protokoll „TFTP“ aus dem WAN verboten war, antwortete der Router bei einem Port-Scan mit einem „TFTP Error (Access Violation)“. Auf das nachfolgende „TFTP Ack“ des Port-Scanners antwortete der Router dann mit der Meldung „Destination unreachable (Port unreachable)“. Es wird jetzt bei einem Port-Scan vom Router direkt die Meldung „Port unreachable“ versendet.
- > Beim Ausführen einer internen Dateisystem-Operation in der Layer 7-Anwendungserkennung (Freigabe einer internen Ressource) konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.
- > Durch eine fehlende Initialisierung beim Start eines LANCOM Routers wurden bei einer SNMP-Abfrage alle Schnittstellen, welche beim Start deaktiviert waren, als aktiv angezeigt.
- > Wenn nur eine DSL-Gegenstelle konfiguriert und aktiv war, enthielten MLPPP-Pakete keinen Multilink-Header, was zur Folge hatte, dass diese Pakete immer auf dem ersten Kanal (Master-Kanal) gesendet wurden.
- > Beim Betrieb eines LANCOM Routers als VDSL-Modem stellte die Bridge nach kurzer Zeit den Betrieb ein. In der Folge war die Internetverbindung nicht mehr funktional.
- > Bei einer Unterbrechung der ADSL-Verbindung (z.B. durch Zwangstrennung) wurde die Internet-Verbindung in einigen Fällen nicht mehr aufgebaut. Dieses Verhalten trat auf, wenn auf einer ADSL-Leitung eine VDSL-Gegenstelle (mit VDSL als Layer 1) verwendet wurde.
- > Bei Verwendung einer Plain-Ethernet-Verbindung (IPoE oder DHCPoE) schlug das ICMP-Polling fehl, wenn als Absende-Adresse ein Netzwerk verwendet wurde, an dessen zugewiesenem Ethernet-Port kein Kabel gesteckt war. In der Folge konnte die Plain-Ethernet-Verbindung nicht aufgebaut werden.

VPN

- › In großen Szenarien wurde die Aufbaugeschwindigkeit von VPN-Tunneln auf zentralseitigen VPN-Gateways verbessert.
- › In der VPN-Status-Tracer-Ausgabe wurde bei der Phase 2 SA-Aushandlung einer IKEv1-Verbindung ein Begriff aus der IKEv2-Technologie verwendet.
- › Beim gleichzeitigen Auf- und Abbau einer IKEv2-Verbindung mit vereinfachter Einwahl konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.

WLAN

- › Wenn im Pfad „Setup / Public-Spot-Module / Brute-Force-Protection“ die Anzahl der „Max-Login-Tries“ auf 0 gesetzt wurde, und die Brute-Force-Detection-Funktion somit deaktiviert war, griff die Funktion weiterhin und ein Public Spot Benutzer konnte sich nicht am System anmelden.
- › Bei Verwendung eines Access Points mit zwei 802.11ac WLAN-Modulen (IAP-822, OAP-822 und OAP-830) kam es bei einem Wechsel eines WLAN-Clients zwischen den beiden WLAN-Interfaces zu einem unvermittelten Neustart, wenn der WLAN-Client sich nicht vom WLAN abgemeldet hat bzw. abgemeldet wurde, da der falsche Interface-Pointer zugewiesen wurde.

VoIP

- › Es konnte nach einem Neustart des Routers vereinzelt dazu kommen, dass eingehende Rufe auf einer IPv6-SIP-Providerleitung nicht signalisiert wurden. Erst nachdem der Voice Call Manager deaktiviert und wieder aktiviert wurde, funktionierte die Telefonie.
- › In einem Szenario, in dem alle IP-Netze und Routing-Einträge mit Routing-Tags versehen waren, konnte es in bestimmten Konstellationen dazu kommen, dass es bei einer Telefonie über den Voice Call Manager zu einer einseitigen Sprachverbindung kam. Es wurde nun die Möglichkeit implementiert, eine Loopback-Adresse (Absende-Adresse) pro SIP-Leitung zu konfigurieren. Über diese kann nun explizit der ausgehende Weg definiert werden.
- › Der Voice Call Manager überprüfte bei Verwendung von TLS zur Authentifizierung bisher nicht den Servernamen, der in der SIP-Domäne/Realm hinterlegt wurde. In der Folge wurde die SIP-Registrierung auch dann durchgeführt, wenn der Servername in der SIP-Domäne/Realm nicht dem Servernamen im Zertifikat entsprach.

LCOS-Änderungen zu 10.20.0097 RC1

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 Readsript-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.

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.