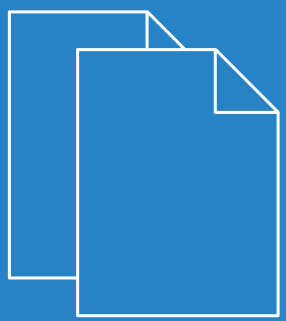
SICHER. **VERNETZT.**

LCOS LX 5.36

Addendum



04/2022

LANCOM Systems

Inhalt

Copyright

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS LX) finden Sie über die Kommandozeile mit dem Befehl `show 3rd-party-licenses`. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Wenden Sie sich hierzu via E-Mail an *gpl@lancom.de*.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS LX-Version 5.36

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 5.36 gegenüber der vorherigen Version.

2 Anpassung der Admin-Passwort-Kriterien

Ab LCOS LX 5.36 muss ein im Rahmen der WEBconfig-Erstinbetriebnahme neu vergebenes Admin-Passwort die folgenden Kriterien erfüllen:

- mindestens 8 Zeichen
- mindestens ein Buchstabe
- mindestens eine Ziffer
- mindestens ein Sonderzeichen

3 Verzögerter Neustart

Das Kommando `do /Other/Delayed-Reboot [<seconds>]` führt einen Neustart des Gerätes nach der angegebenen Anzahl von Sekunden aus.

Mit dem Kommando `do /Other/Cancel-Delayed-Reboot` lässt sich der so geplante Neustart innerhalb der angegebenen Zeitspanne wieder abbrechen.

Diese Funktion wird für die Zusammenarbeit mit einigen Managementsystemen verwendet.

3.1 Ergänzungen im Setup-Menü

3.1.1 Delayed-Reboot

Mit dieser Aktion starten Sie das Gerät verzögert neu. Die Verzögerung wird als Parameter in Sekunden angegeben.

Beispiel: `do Delayed-Reboot 30`

SNMP-ID:

–

Pfad Konsole:

Other

3.1.2 Cancel-Delayed-Reboot

Mit dieser Aktion brechen Sie einen mit `do Delayed-Reboot` eingeleiteten verzögerten Neustart innerhalb der Verzögerungszeit ab.

Beispiel: `do Cancel-Delayed-Reboot`

SNMP-ID:

–

Pfad Konsole:

Other

4 writeconfig-Kommando

Nach Ausführen des writeconfig-Kommandos kann der CLI-Sitzung eine Konfiguration im LCF-Format übergeben werden, die anschließend vom Gerät angewandt und persistiert wird.

Durch Anhängen des Parameters `noflash` wird die übergebene Konfiguration nicht persistiert. Dies kann durch das nachträgliche Ausführen des `flash`-Befehls erfolgen. Dieses Feature ist hautpsächlich für die Zusammenarbeit mit einigen Managementsystemen relevant.

Befehl	Beschreibung
`writeconfig [noflash]`	Schreibt eine neue Konfiguration in Form einer LCF-Datei in das Gerät. Das System interpretiert alle folgenden Zeilen solange als Konfigurationswerte, bis zwei Leerzeilen auftreten. Dies wird z. B. von Managementsystemen genutzt. Mögliche Optionsschalter sind: › `noflash`: Die übergebene Konfiguration wird nicht persistiert. Dies kann durch das nachträgliche Ausführen des `flash`-Befehls erfolgen.

5 Untagged-VLAN für weitere Ethernet-Ports

Besitzt ein Gerät mehr als einen Ethernet-Port, können die weiteren Ethernet-Ports optional mit einen Untag-VLAN konfiguriert werden. Das Untag-VLAN wird ohne VLAN-Tag auf dem weiteren LAN-Port verwendet und dient z. B. dazu, weitere Netzwerkgeräte in das Netzwerk einzubinden, die ihrerseits nicht VLAN-fähig sind. Der weitere Ethernet-Port agiert somit als Access-Port.

Die folgenden Access Points mit LCOS LX sind mit mehr als einem Ethernet-Port ausgestattet und unterstützen somit dieses Feature:

- LANCOM LW-500
- LANCOM LX-6400
- LANCOM LX-6402
- LANCOM OW-602

5.1 Ergänzungen im Setup-Menü

5.1.1 Untagged-VLAN

Besitzt ein Gerät mehr als einen Ethernet-Port, können die weiteren Ethernet-Ports optional mit einen Untag-VLAN konfiguriert werden. Das Untag-VLAN wird ohne VLAN-Tag auf dem weiteren LAN-Port verwendet und dient z.B. dazu, weitere Netzwerkgeräte in das Netzwerk einzubinden, die ihrerseits nicht VLAN-fähig sind. Der weitere Ethernet-Port agiert somit als Access-Port. Die Untag-Ports und deren VLAN-TAG werden in dieser Tabelle angegeben.

SNMP-ID:

2.70.8

Pfad Konsole:

Setup > **IP-Configuration**

Port

Geben Sie einen Port für Untag-VLAN an.

SNMP-ID:

2.70.8.1

Pfad Konsole:

Setup > **IP-Configuration** > **Untagged-VLAN**

Mögliche Werte:

ETH1
ETH2
…

VLAN

Geben Sie eine VLAN-ID für Untag-VLAN an.

SNMP-ID:

2.70.8.2

Pfad Konsole:

Setup > **IP-Configuration** > **Untagged-VLAN**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

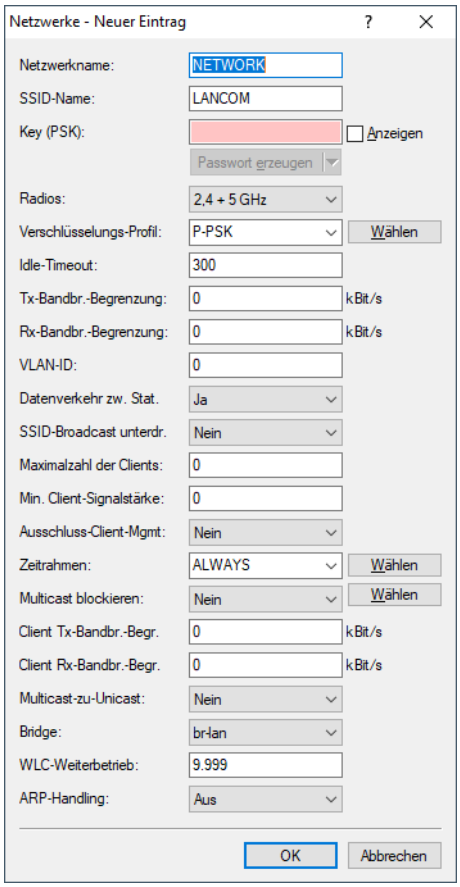
Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

6 ARP-Handling

Clients im WLAN, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der „ARP-Behandlung" übernimmt der Access Point diese Aufgabe und beantwortet die ARP-Anfragen an Stelle der Stationen im Stromsparmodus. In großen Netzen wird hierdurch ebenfalls die Mediumszeit effizienter genutzt, da ARP-Anfragen und -Antworten nicht mehr an den WLAN-Client gesendet werden müssen, sondern schon stellvertretend vom Access Point beantwortet werden.

Konfiguration in LANconfig

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** das ARP-Handling.



ARP-Handling

Clients im WLAN, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der „ARP-Behandlung" übernimmt der Access Point diese Aufgabe und beantwortet die ARP-Anfragen an Stelle der Stationen im Stromsparmodus. In großen Netzen wird hierdurch ebenfalls die Mediumszeit effizienter genutzt, da ARP-Anfragen und -Antworten nicht mehr an den WLAN-Client gesendet werden müssen, sondern schon stellvertretend vom Access Point beantwortet werden.

Der LCOS LX Access Point ermittelt die Zuordnung zwischen IP-Adresse und MAC-Adresse aus den DHCP-Nachrichten, die zwischen WLAN-Client und DHCP-Server ausgetauscht werden. Ist die Zuordnung

bekannt, werden ARP-Anfragen durch den Access Point beantwortet und nicht mehr an den Client weitergeleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „An“ ARP-Anfragen trotzdem in das WLAN geleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „Strikt“ ARP-Anfragen nicht in das WLAN geleitet. Dies bedeutet zum Beispiel, dass zu WLAN-Clients mit festen IP-Adressen (kein DHCP) keine Verbindung vom LAN aus initiiert werden kann. In diesem Fall sollte dieses Feature nicht verwendet werden.

Aus

ARP-Behandlung ausgeschaltet. ARP-Anfragen werden immer in das WLAN geleitet.

An

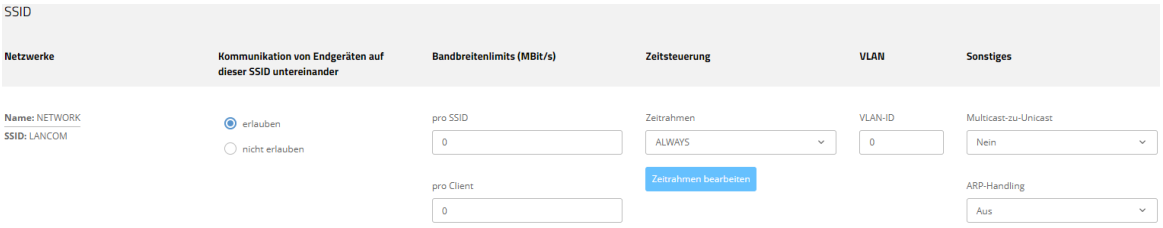
ARP-Behandlung eingeschaltet. ARP-Anfragen werden nur in das WLAN geleitet, wenn keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden konnte.

Strikt

ARP-Behandlung eingeschaltet. ARP-Anfragen werden in keinem Fall in das WLAN geleitet.

Konfiguration in WEBconfig

Konfigurieren Sie unter **WLAN-Konfiguration** > **SSID** das ARP-Handling.



Sonstiges

ARP-Handling

Clients im WLAN, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der „ARP-Behandlung“ übernimmt der Access Point diese Aufgabe und beantwortet die ARP-Anfragen an Stelle der Stationen im Stromsparmodus. In großen Netzen wird hierdurch ebenfalls die Mediumszeit effizienter genutzt, da ARP-Anfragen und -Antworten nicht mehr an den WLAN-Client gesendet werden müssen, sondern schon stellvertretend vom Access Point beantwortet werden.

Der LCOS LX Access Point ermittelt die Zuordnung zwischen IP-Adresse und MAC-Adresse aus den DHCP-Nachrichten, die zwischen WLAN-Client und DHCP-Server ausgetauscht werden. Ist die Zuordnung bekannt, werden ARP-Anfragen durch den Access Point beantwortet und nicht mehr an den Client weitergeleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „An“ ARP-Anfragen trotzdem in das WLAN geleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „Strikt“ ARP-Anfragen nicht in das WLAN geleitet. Dies bedeutet zum Beispiel, dass zu

WLAN-Clients mit festen IP-Adressen (kein DHCP) keine Verbindung vom LAN aus initiiert werden kann. In diesem Fall sollte dieses Feature nicht verwendet werden.

Aus

ARP-Behandlung ausgeschaltet. ARP-Anfragen werden immer in das WLAN geleitet.

An

ARP-Behandlung eingeschaltet. ARP-Anfragen werden nur in das WLAN geleitet, wenn keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden konnte.

Strikt

ARP-Behandlung eingeschaltet. ARP-Anfragen werden in keinem Fall in das WLAN geleitet.

6.1 Ergänzungen im Setup-Menü

6.1.1 ARP-Handling

Clients im WLAN, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der „ARP-Behandlung" übernimmt der Access Point diese Aufgabe und beantwortet die ARP-Anfragen an Stelle der Stationen im Stromsparmodus. In großen Netzen wird hierdurch ebenfalls die Mediumszeit effizienter genutzt, da ARP-Anfragen und -Antworten nicht mehr an den WLAN-Client gesendet werden müssen, sondern schon stellvertretend vom Access Point beantwortet werden.

Der LCOS LX Access Point ermittelt die Zuordnung zwischen IP-Adresse und MAC-Adresse aus den DHCP-Nachrichten, die zwischen WLAN-Client und DHCP-Server ausgetauscht werden. Ist die Zuordnung bekannt, werden ARP-Anfragen durch den Access Point beantwortet und nicht mehr an den Client weitergeleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „An" ARP-Anfragen trotzdem in das WLAN geleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „Strikt" ARP-Anfragen nicht in das WLAN geleitet. Dies bedeutet zum Beispiel, dass zu WLAN-Clients mit festen IP-Adressen (kein DHCP) keine Verbindung vom LAN aus initiiert werden kann. In diesem Fall sollte dieses Feature nicht verwendet werden.

SNMP-ID:

2.20.1.28

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

Off

ARP-Behandlung ausgeschaltet. ARP-Anfragen werden immer in das WLAN geleitet.

On

ARP-Behandlung eingeschaltet. ARP-Anfragen werden nur in das WLAN geleitet, wenn keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden konnte.

Strict

ARP-Behandlung eingeschaltet. ARP-Anfragen werden in keinem Fall in das WLAN geleitet.

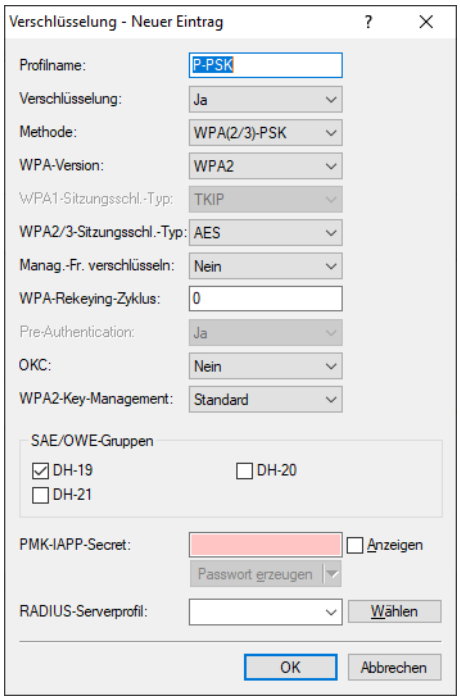
Default-Wert:

Off

7 Opportunistic Key Caching

Konfiguration in LANconfig

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** das Opportunistic Key Caching.



OKC (Opportunistic Key Caching)

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

Authentifizierung von WLAN-Clients über EAP und 802.1X ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation Anwendung. Der Nachteil der Authentifizierung über 802.1X ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und Access Point sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der Access Point Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen Access Points im WLAN-Netzwerk verarbeiten muss.

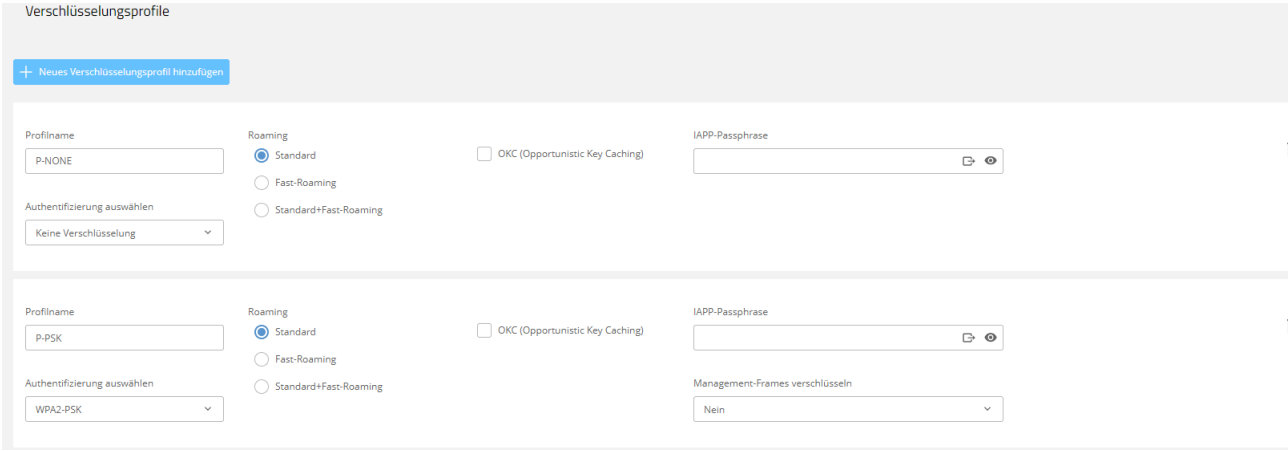
Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLAN-Controller (WLC) oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access Point in der Erwartung, dass dieser OKC aktiviert hat (deshalb „opportunistisch“). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1X-Authentifizierung aus.

Ein LANCOM Access Point kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

In von der LANCOM Management Cloud (LMC) verwalteten Netzen oder Netzen aus Standalone-Access-Points werden die PMKs über das IAPP-Protokoll übertragen. In LMC-verwalteten Netzen wird das IAPP automatisch konfiguriert. Sorgen Sie in Netzen aus Standalone-Access-Points dafür, dass das PMK-IAPP-Secret auf allen Access Points des Netzwerks konfiguriert und identisch ist.

Konfiguration in WEBconfig

Konfigurieren Sie unter **WLAN-Konfiguration** > **Verschlüsselung** das Opportunistic Key Caching.



OKC (Opportunistic Key Caching)

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

Authentifizierung von WLAN-Clients über EAP und 802.1X ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation Anwendung. Der Nachteil der Authentifizierung über 802.1X ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und Access Point sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der Access Point Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen Access Points im WLAN-Netzwerk verarbeiten muss.

Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLAN-Controller (WLC) oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access Point in der Erwartung, dass dieser OKC aktiviert hat (deshalb „opportunistisch“). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1X-Authentifizierung aus.

Ein LANCOM Access Point kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

In von der LANCOM Management Cloud (LMC) verwalteten Netzen oder Netzen aus Standalone-Access-Points werden die PMKs über das IAPP-Protokoll übertragen. In LMC-verwalteten Netzen wird das IAPP automatisch konfiguriert. Sorgen Sie in Netzen aus Standalone-Access-Points dafür, dass das PMK-IAPP-Secret auf allen Access Points des Netzwerks konfiguriert und identisch ist.

7.1 Ergänzungen im Setup-Menü

7.1.1 OKC

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

SNMP-ID:

2.20.3.17

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

OKC ist aktiviert.

Yes

OKC ist nicht aktiviert.

8 LANCOM Layer 2 Management Protokoll (LL2M)

Ab LCOS LX 5.36 können Sie LL2M zur Konfiguration nutzen. Die Einstellungen zur Konfiguration finden Sie in der WEBconfig unter **Systemkonfiguration** > **LL2M-Konfiguration**.

8.1 LL2M-Konfiguration

Die Einstellungen für LL2M finden Sie in der WEBconfig unter **Systemkonfiguration** > **LL2M-Konfiguration**.

Betrieb

Alle Wege zur Konfiguration eines Geräts setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem Gerät voraus. Egal ob LANconfig, WEBconfig oder SSH – ohne IP-Verbindung können keine Befehle zur Konfiguration an das Gerät übertragen werden. Im Falle einer Fehlkonfiguration der TCP/IP-Einstellungen oder der VLAN-Parameter kann es vorkommen, dass diese benötigte IP-Verbindung nicht mehr hergestellt werden kann. In diesen Fällen hilft nur der Zugriff über die serielle Konfigurationsschnittstelle, die allerdings nicht bei allen Geräten verfügbar ist oder ein Reset des Gerätes auf den Auslieferungszustand. Beide Möglichkeiten setzen aber den physikalischen Zugriff auf das Gerät voraus, der z. B. bei der verdeckten Montage von Access Points nicht immer gegeben ist oder in größeren Szenarien erheblichen Aufwand darstellen kann.

Um auch ohne IP-Verbindung einen Konfigurationszugriff auf ein Gerät zu ermöglichen, wird das **LANCOM Layer 2 Management Protokoll (LL2M)** verwendet. Dieses Protokoll benötigt nur eine Verbindung auf Layer 2, also auf dem direkt oder über Layer-2-Switches angebundenen Ethernet, um eine Konfigurationssitzung aufzubauen. LL2M-Verbindungen werden auf LAN- oder WLAN-Verbindungen unterstützt, nicht jedoch über das WAN. Die Verbindungen über LL2M sind passwortgeschützt und gegen Replay-Attacken resistent.

LL2M etabliert dazu eine Client-Server-Struktur: Der LL2M-Client schickt Anfragen oder Befehle an den LL2M-Server, der die Anfragen beantwortet oder die Befehle ausführt. Sowohl der LL2M-Client als auch der LL2M-Server sind im LCOS LX integriert. Die Befehle des LL2M-Clients werden über die Konsole oder die WEBconfig ausgeführt.

Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die Befehle `LL2Mdetect` bzw. `LL2Mexec`.

Aktivieren Sie hier LL2M.

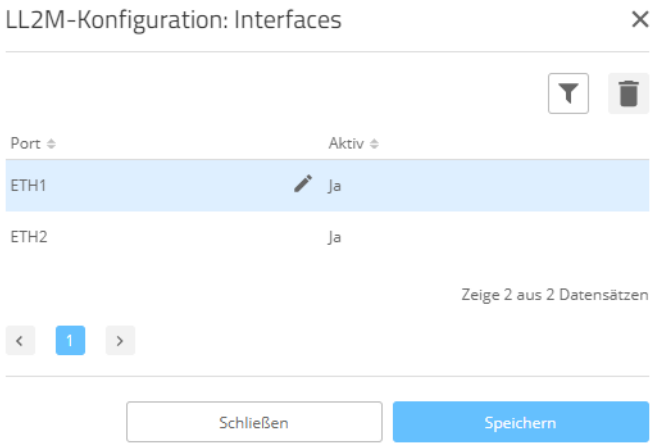
Access Points vom Typ LANCOM LW-500 sind nur über LL2M auffind- und konfigurierbar, wenn LL2M-Pakete den Access Point mit einem VLAN-Tag erreichen, welches in der Konfiguration des Access Points enthalten ist (WLAN-SSID-Konfiguration oder Management-VLAN-Konfiguration).

Status

Zeigt den Status der aktuellen LL2M-Konfiguration an.

Interfaces

Hier können Sie die Interfaces bzw. Ethernet-Ports angeben, auf denen Sie den LL2M-Server erreichen können. Voreingestellt ist die Erreichbarkeit auf allen Ethernet-Ports.



CLI-Befehle `LL2Mdetect` und `LL2Mexec`

Befehl	Beschreibung
`ll2mdetect`	LL2Mdetect erkennt LL2M-fähige Geräte im Netzwerk. Mit diesem Befehl schickt der LL2M-Client eine SYSINFO-Anfrage an den LL2M-Server. Der Server sendet daraufhin seine Systeminformationen wie Hardware, Seriennummer etc. zur Anzeige an den Client zurück. Der LL2Mdetect-Befehl lässt sich mit folgenden Parametern einschränken: **`-a <MAC-Adresse>`** Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse geben Sie in der Form `00a057010203`, `00-a0-57-01-02-03` oder `00:a0:57:01:02:03` an. Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder via `-b` alternativ als Broadcast) an alle LL2M-fähigen Geräte. Einzelne Stellen der MAC-Adresse können mit einem `*` oder `x` als Platzhalter besetzt werden, um Gruppen von MAC-Adressen anzusprechen, z. B. `00-a0-57-xx-xx-xx` für alle Geräte-MAC-Adressen.

Befehl	Beschreibung
	In einer Befehlszeile mit mehreren Parametern **muss** `-a` der abschließende Parameter sein. Eine andere Reihenfolge ist nicht zulässig. **`-b`** Versendet die LL2Mdetect-Anfrage explizit als Broadcast und nicht als Multicast. **`-f <Version>`** Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein. **`-r <Hardware-Release>`** Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein. **`-s <Serialnumber>`** Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein. **`-t <Hardware-Type>`** Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein. **`-v <VLAN-ID>`** Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet. Die Befehlszeile `ll2mdetect -r A` zum Beispiel versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release 'A'. Die Antwort des LL2M-Servers enthält dann die folgenden Angaben: › Name des Gerätes › Gerätetyp › Seriennummer › MAC-Adresse › Hardware-Release › Firmware-Version mit Datum
`ll2mexec`	Mit `ll2mexec` können Befehle an per `ll2mdetect` gefundene Geräte geschickt werden oder interaktive Konsolensessions aufgebaut werden. Mit diesem Befehl schickt der LL2M-Client ein einzeiliges Kommando zur Ausführung an den LL2M-Server. Mehrere Kommandos lassen sich durch Semikola getrennt in einem LL2M-Befehl kombinieren. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes zur Anzeige an den LL2M-Client übertragen. Der LL2Mexec-Befehl entspricht folgender Syntax: `ll2mexec <User>[:<Password>]@<MAC-Address>`

Befehl	Beschreibung
	Der LL2Mexec-Befehl lässt sich mit folgenden Parametern einschränken: **`-i <(W)LAN-Interface>`** Versendet den LL2Mexec-Befehl nur über das angegebene (W)LAN-Interface. **`-v <VLAN-ID>`** Versendet den LL2Mexec-Befehl nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet. Die Befehlszeile `ll2mexec root@00a057010203 set /setup/name MyDevice` zum Beispiel meldet den LL2M-Client als 'root' auf dem LL2M-Server mit der MAC-Adresse '00a057010203' an. Da das Passwort weggelassen wurde, sucht das Gerät zunächst nach dem entsprechenden Nutzernamen in der lokalen Datenbank und setzt automatisch das für diesen Nutzer gespeicherte Passwort ein. Wird auch der Nutzername weggelassen, werden die Anmeldedaten des aktuell für die CLI-Sitzung registrierten Nutzers verwendet. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert 'MyDevice'.

8.2 Ergänzungen im Setup-Menü

8.2.1 LL2M

Alle Wege zur Konfiguration eines Geräts setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem Gerät voraus. Egal ob LANconfig, WEBconfig oder SSH – ohne IP-Verbindung können keine Befehle zur Konfiguration an das Gerät übertragen werden. Im Falle einer Fehlkonfiguration der TCP/IP-Einstellungen oder der VLAN-Parameter kann es vorkommen, dass diese benötigte IP-Verbindung nicht mehr hergestellt werden kann. In diesen Fällen hilft nur ein Reset des Gerätes auf den Auslieferungszustand. Diese Möglichkeit setzt aber den physikalischen Zugriff auf das Gerät voraus, der z. B. bei der verdeckten Montage von Access Points nicht immer gegeben ist oder in größeren Szenarien erheblichen Aufwand darstellen kann.

Um auch ohne IP-Verbindung einen Konfigurationszugriff auf ein Gerät zu ermöglichen, wird das **LANCOM Layer 2 Management Protokoll (LL2M)** verwendet. Dieses Protokoll benötigt nur eine Verbindung auf Layer 2, also auf dem direkt oder über Layer-2-Switches angebundenen Ethernet, um eine Konfigurationssitzung aufzubauen. LL2M-Verbindungen werden auf LAN- oder WLAN-Verbindungen unterstützt, nicht jedoch über das WAN. Die Verbindungen über LL2M sind passwortgeschützt und gegen Replay-Attacken resistent.

LL2M etabliert dazu eine Client-Server-Struktur: Der LL2M-Client schickt Anfragen oder Befehle an den LL2M-Server, der die Anfragen beantwortet oder die Befehle ausführt. Sowohl der LL2M-Client als auch der LL2M-Server sind im LCOS LX integriert. Die Befehle des LL2M-Clients werden über die Konsole oder die WEBconfig ausgeführt.

Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die Befehle `LL2Mdetect` bzw. `LL2Mexec`. Siehe *Konsole – Befehlsübersicht*.

Zum Ausführen der Befehle für den LL2M-Client müssen Sie über Root-Rechte auf dem LL2M-Server verfügen.

Access Points vom Typ LANCOM LW-500 sind nur über LL2M auffind- und konfigurierbar, wenn LL2M-Pakete den Access Point mit einem VLAN-Tag erreichen, welches in der Konfiguration des Access Points enthalten ist (WLAN-SSID-Konfiguration oder Management-VLAN-Konfiguration).

Dieses Menü enthält die Einstellungen für das LANCOM Layer-2 Management.

SNMP-ID:

2.50

Pfad Konsole:

Setup

Operating

Schaltet den LL2M-Server ein oder aus.

SNMP-ID:

2.50.1

Pfad Konsole:

Setup > LL2M

Mögliche Werte:

No

LL2M-Server ist ausgeschaltet.

Yes

LL2M-Server ist eingeschaltet.

Default-Wert:

Yes

Interfaces

Hier können Sie die Interfaces bzw. Ethernet-Ports angeben, auf denen Sie den LL2M-Server erreichen können. Voreingestellt ist die Erreichbarkeit auf allen Ethernet-Ports. Ein Zugang über WLAN ist nicht vorgesehen.

SNMP-ID:

2.50.2

Pfad Konsole:

Setup > LL2M

Port

Portbezeichnung, z.B. ETH1.

SNMP-ID:

2.50.2.1

Pfad Konsole:

Setup > **LL2M** > **Interfaces**

Mögliche Werte:

max. 5 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Active

Schaltet den LL2M-Server für diesen Port ein oder aus.

SNMP-ID:

2.50.2.2

Pfad Konsole:

Setup > **LL2M** > **Interfaces**

Mögliche Werte:

No
Yes

Default-Wert:

Yes