LCOS LX 6.10

Addendum

02/2023

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.

 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.

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 6.10

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 6.10 gegenüber der vorherigen Version.

2 Unterstützung für Wi-Fi 6E / das 6 GHz-Band

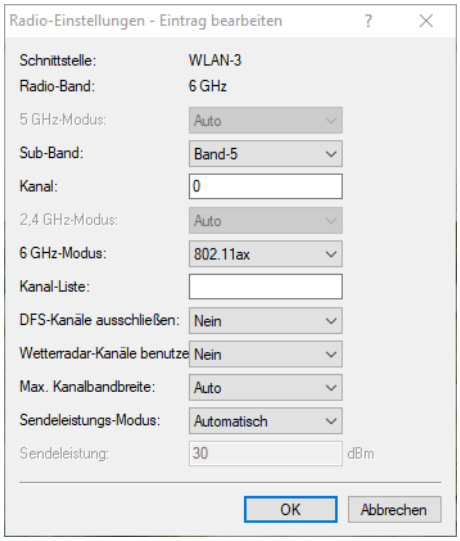
Ab LCOS LX 6.10 wird die Verwendung des 6 GHz-Frequenzbands für WLAN unterstützt.

Folgende Einstellungsmöglichkeiten wurden für die Verwendung von 6 GHz angepasst bzw. erweitert:

Wireless-LAN > **WLAN-Netzwerke** > **Radio-Einstellungen**

Auf kompatiblen Access Points enthält diese Tabelle einen zusätzlichen Eintrag „WLAN-3" zur Konfiguration des 6 GHz-WLAN-Radios.

Wie bei den 2,4 GHz- und 5 GHz-Radios ist das Frequenzband nicht veränderbar. Das Radio WLAN-3 unterstützt nur das 6 GHz-Band.



Sub-Band

Das Sub-Band „Band-5" wurde hinzugefügt. Die Bezeichnung Band-5 orientiert sich an der U-NII-Nomenklatur der FCC und entspricht dem Band U-NII-5. In der EU ist im Rahmen des 6 GHz-Bands lediglich der Frequenzbereich 5.925–6.425 MHz für WLAN freigegeben (was Band-5, bzw. U-NII-5 entspricht). Daher ist aktuell in LCOS LX lediglich das Sub-Band „Band-5" auswählbar.

Kanal

Im 6 GHz-Band können in LCOS LX folgende Kanäle konfiguriert werden:

1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93

Hierbei handelt es sich um 20 MHz breite Kanäle. Wird eine höhere Kanalbreite als 20 MHz gewählt (Standardeinstellung für das 6 GHz-Band: 160 MHz) wird der hier eingestellte Kanal zum Primärkanal des dann verwendeten breiteren Kanals. Auf diese Weise kann der Primärkanal ebenfalls frei innerhalb eines >20 MHz breiten Kanals gewählt werden – dazu muss lediglich der gewünschte 20 MHz-Kanal eingetragen werden.

6 GHz-Modus

Im 6 GHz-Band wird lediglich der neue 802.11ax-Standard unterstützt. Folglich kann nur dieser ausgewählt werden.

Max. Kanalbandbreite

Im Auto-Modus wird für das 6 GHz-Band immer eine Kanalbandbreite von 160 MHz verwendet (2,4 GHz: 20 MHz; 5 GHz: 80 MHz). Auf Wunsch kann die Kanalbbandreite hier weiter eingeschränkt werden.

Hinweis zur WLAN-Verschlüsselung im 6 GHz-Band

Da im 6 GHz-Band aufgrund des für WLAN vollkommen neuen Frequenzbandes keine Abwärtskompatibilität mit alten Clients notwendig ist, werden veraltete Sicherheitsverfahren nicht unterstützt. Konkret bedeutet dies:

- ausschließliche Verwendung von WPA3 für verschlüsselte Netze. Dementsprechend ist auch kein Transition-Modus bzw. gemischter Modus wie WPA2/3 möglich.
- Verwendung von Enhanced Open für „offene" Netze (die dadurch dennoch eine Verschlüsselung der übertragenen Daten bieten). Offene, unverschlüsselt betriebene SSIDs sind nicht mehr möglich!
- Protected Management Frames müssen verpflichtend genutzt werden

Die o. g. Bedingungen können in der LCOS LX-Konfiguration gesetzt werden. Ist die explizite Konfiguration nicht gewünscht oder möglich (z. B. beim gemischten Betrieb derselben SSID auf mehreren Bändern, was ein häufiger Anwendungsfall ist), werden folgende Anpassungen von LCOS LX dynamisch vorgenommen, sobald eine SSID auf dem 6 GHz-Band verwendet werden soll:

- WPA-Versionen <3 werden automatisch auf WPA3 angepasst
- Enhanced-Open wird für offene Netzwerke aktiviert
- Protected Management Frames wird aktiviert

Hierdurch ist es möglich, bestehende Verschlüsselungsprofile weiter zu verwenden und eine gemeinsame Konfiguration für eine SSID, die zusätzlich auf 6 GHz ausgestrahlt werden soll, zu verwenden. Diese Einstellungen werden dynamisch im Betrieb angepasst, die im Gerät hinterlegte Konfiguration wird also nicht verändert.

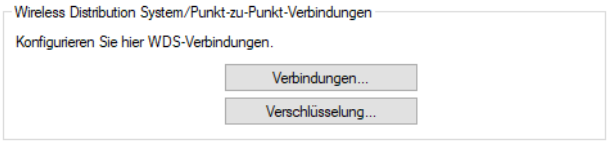
3 Wireless Distribution System (WDS) / Punkt-zu-Punkt-Verbindungen

Mittels des WDS lassen sich Punkt-zu-Punkt-WLAN-Verbindungen zwischen Access Points aufbauen. Diese Verbindungen dienen als kabelloser Backhaul und ermöglichen so die Anbindung von abgesetzt betriebenen Access Points an den Rest des Netzwerks. So lässt sich beispielsweise die WLAN-Abdeckung auch in Bereichen sicher stellen, in denen keine Ethernet-Anbindung von Access Points möglich ist.

Die beteiligten Access Points können wahlweise ihrerseits SSIDs für die WLAN-Client-Anbindung anbieten („Repeater"-Betrieb) oder die kabellose Backhaul-Verbindung mit ihrem Ethernet-Port verbinden (Wireless Bridge).

Mit LCOS LX 6.10 ist der WDS-Betrieb über eine Strecke von maximal 300 Metern validiert.

Die Einstellungen für WDS Ihres Gerätes finden Sie unter **Wireless-LAN** > **WDS**.



Übertragung von WLAN-Netzwerken

Im Rahmen der WLAN-Konfiguration können Sie festlegen, dass bestimmte SSIDs über WDS-Verbindungen übertragen werden. Dies erfolgt unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** im Auswahlfeld **WDS-Verbindung**.

Soll ein Repeater-Betrieb realisiert werden, muss diese Konfiguration ebenso auf dem entfernten via WDS angebundenen Access Point dupliziert werden.

Radio-Einstellungen

Die allgemeinen Radio-Einstellungen, die für den Access Point vorgenommen wurden, gelten auch für WDS-Verbindungen (insbesondere die Einstellung des WLAN-Kanals). Nehmen Sie diese wie gewohnt unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** vor.

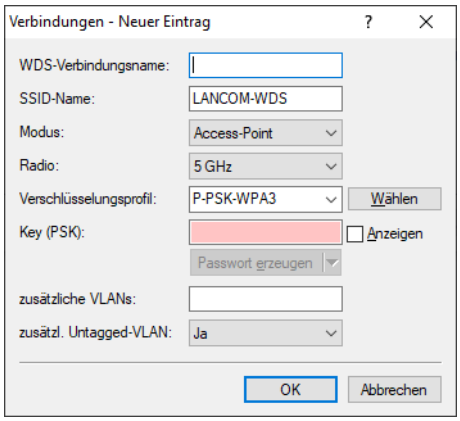
Achten Sie insbesondere darauf, dass eine eventuelle Kanalvorgabe oder Einschränkung auf bestimmte Unterbänder auf beiden Seiten der WDS-Verbindung übereinstimmt, damit die Verbindung aufgebaut werden kann. Alternativ kann auf beiden Seiten die automatische Kanalwahl verwendet werden. In diesem Fall sucht die Station über alle erlaubten Kanäle, bis der WDS-Partner gefunden wird.

Unterstützte LANCOM Geräte

- LX-6500(E)
- LX-6400
- LX-6402
- LW-600
- OX-6400
- OX-6402
- OW-602
- LX-6200(E)

3.1 Verbindungen

Konfigurieren Sie unter **Wireless-LAN** > **WDS** > **Verbindungen** alle generellen Einstellungen rund um die WDS-Verbindung. Fügen Sie je WDS-Verbindung eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.



WDS-Verbindungsname

Der Name der Verbindung. Wird für die weitere Referenzierung in der Gerätekonfiguration verwendet.

SSID-Name

Der Name der speziellen SSID, die für die WDS-Verbindung verwendet wird. Dieser Name muss auf beiden Seiten der Verbindung übereinstimmen.

Modus

Im Rahmen einer WDS-Verbindung gibt es zwei Rollen: Access-Point und Station. Der als Station konfigurierte Partner sucht anhand der oben konfigurierten SSID den als Access-Point konfigurierten Partner und initiiert die Verbindung.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Stationen zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget" verwendet.

Es können beliebig viele WDS-Verbindungen im Access-Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden. Verbindungen im Access-Point-Modus und Station-Modus (von letzterer nur eine) können gleichzeitig auf demselben Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten" ausreichend ist.

Radio

Das Frequenzband, welches für die WDS-Verbindung genutzt werden soll. Aus Kapazitätsgründen empfiehlt sich die Verwendung von 5 GHz oder 6 GHz (je nach Hardware-Fähigkeiten des verwendeten Gerätemodells).

Verschlüsselungsprofil

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll. Voreingestellt und empfohlen ist die ausschließliche Verwendung von WPA3.

Key (PSK)

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird.

zusätzliche VLANs

Im Rahmen der WLAN-Konfiguration ist es möglich, einzelne SSIDs mit WDS-Verbindungen zu verknüpfen. Diese werden dann gebridget über die WDS-Verbindung zur Verfügung gestellt. Sollen zusätzliche, z. B. über Ethernet transportierte VLANs ebenfalls übertragen werden, können diese hier eingetragen werden (kommaseparierte Liste von VLAN-IDs [0-4095]).

zusätzl. untagged VLAN

Untagged-Pakete sollen übertragen werden.

3.2 Verschlüsselung

Konfigurieren Sie unter **Wireless-LAN** > **WDS** > **Verschlüsselung** alle Einstellungen rund um die Verschlüsselung und Authentisierung des Wireless Distribution Systems.

Für WDS-Verbindungen empfehlen wir, ausschließlich WPA3 zu verwenden um höchste Sicherheit zu garantieren.

Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-PSK-WPA2

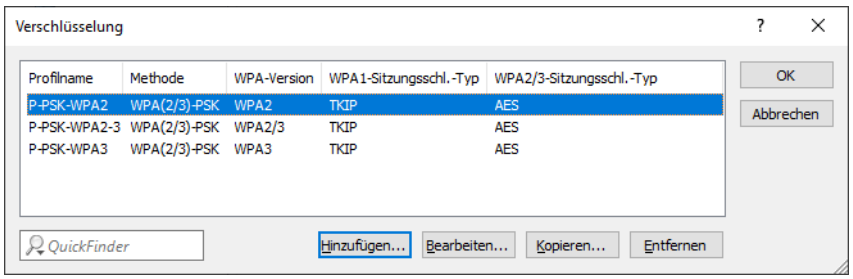
Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.



Profilname

Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.

Methode

Konfigurieren Sie hier die Verschlüsselungsmethode. Folgende Methoden stehen zur Auswahl:

WPA

WPA(2/3)-PSK: WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal

WPA-Version

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode. Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden WPA(2)-PSK und WPA(2)-802.1X verwendet werden. Folgende Versionen stehen zur Auswahl:

- WPA1: Die WPA-Version 1 wird exklusiv verwendet.
- WPA2: Die WPA-Version 2 wird exklusiv verwendet.
- WPA3: Die WPA-Version 3 wird exklusiv verwendet.
- WPA1/2: Abhängig von den Fähigkeiten des Clients wird die WPA-Version 1 oder 2 verwendet.
- WPA2/3: Abhängig von den Fähigkeiten des Clients wird die WPA-Version 2 oder 3 verwendet.

WPA1-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

WPA2/3-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 und 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

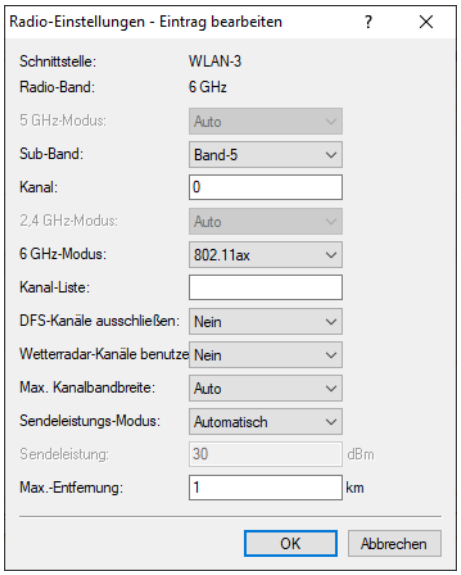
Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

3.3 Maximale Entfernung

Zusätzlich haben Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** die Möglichkeit, die maximale Entferung zu einer WLAN-Station anzugeben.



Max. Entfernung

Geben Sie hier die Distanz zur am weitesten entfernten WLAN-Station ein (z. B. zu einem WDS-Partner).

Anhand dieser Einstellung wird der interne Timeout für WLAN-ACK-Pakete so weit erhöht, dass Pakete von einer weit entfernten Station noch verarbeitet werden können. Default ist 1 Kilometer.

3.4 Ergänzungen im Setup-Menü

3.4.1 WDS-Link

Hier können Sie festlegen, dass bestimmte SSIDs über WDS-Verbindungen übertragen werden. Referenzieren Sie dazu hier einen Eintrag aus *2.20.13.1.1 Link-Name* auf Seite 12.

Soll ein Repeater-Betrieb realisiert werden, muss diese Konfiguration ebenso auf dem entfernten via WDS angebundenen Access Point dupliziert werden.

SNMP-ID:

2.20.1.32

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.4.2 WDS

Mittels des Wireless Distribution System (WDS) lassen sich Punkt-zu-Punkt-WLAN-Verbindungen zwischen Access Points aufbauen. Diese Verbindungen dienen als kabelloser Backhaul und ermöglichen so die Anbindung von abgesetzt betriebenen Access Points an den Rest des Netzwerks. So lässt sich beispielsweise die WLAN-Abdeckung auch in Bereichen sicher stellen, in denen keine Ethernet-Anbindung von Access Points möglich ist.

Die beteiligten Access Points können wahlweise ihrerseits SSIDs für die WLAN-Client-Anbindung anbieten („Repeater"-Betrieb) oder die kabellose Backhaul-Verbindung mit ihrem Ethernet-Port verbinden (Wireless Bridge).

SNMP-ID:

2.20.13

Pfad Konsole:

Setup > **WLAN**

Links

Konfigurieren Sie in dieser Tabelle alle generellen Einstellungen rund um die auszustrahlenden WLAN-Netzwerke (SSIDs). Fügen Sie je WLAN-Netzwerk eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

SNMP-ID:

2.20.13.1

Pfad Konsole:

Setup > **WLAN** > **WDS**

Link-Name

Der Name der Verbindung. Wird für die weitere Referenzierung in der Gerätekonfiguration verwendet.

SNMP-ID:

2.20.13.1.1

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

SSID-Name

Der Name der speziellen SSID, die für die WDS-Verbindung verwendet wird. Dieser Name muss auf beiden Seiten der Verbindung übereinstimmen.

SNMP-ID:

2.20.13.1.2

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

Mode

Im Rahmen einer WDS-Verbindung gibt es zwei Rollen: Access-Point und Station. Der als Station konfigurierte Partner sucht anhand der oben konfigurierten SSID den als Access-Point konfigurierten Partner und initiiert die Verbindung.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Stationen zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget" verwendet.

Es können beliebig viele WDS-Verbindungen im Access-Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten" ausreichend ist.

SNMP-ID:

2.20.13.1.3

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

Access-Point
Station

Radio

Das Frequenzband, welches für die WDS-Verbindung genutzt werden soll. Aus Kapazitätsgründen empfiehlt sich die Verwendung von 5 GHz oder 6 GHz (je nach Hardware-Fähigkeiten des verwendeten Gerätemodells).

SNMP-ID:

2.20.13.1.4

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

2.4GHz

Die SSID wird nur auf der Frequenz 2,4 GHz ausgestrahlt.

5GHz

Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

6GHz

Die SSID wird nur auf der Frequenz 6 GHz ausgestrahlt.

Encryption-Profile

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll. Voreingestellt und empfohlen ist die ausschließliche Verwendung von WPA3.

SNMP-ID:

2.20.13.1.5

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Encryption-Key

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird.

SNMP-ID:

2.20.13.1.6

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

Additional-VLANs

Im Rahmen der WLAN-Konfiguration ist es möglich, einzelne SSIDs mit WDS-Verbindungen zu verknüpfen. Diese werden dann gebridget über die WDS-Verbindung zur Verfügung gestellt. Sollen zusätzliche, z. B. über Ethernet transportierte VLANs ebenfalls übertragen werden, können diese hier eingetragen werden (kommaseparierte Liste von VLAN-IDs [0-4095]).

SNMP-ID:

2.20.13.1.8

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[0-9],`

Additional-Untagged-VLAN

Nicht-VLAN-getaggte Pakete werden über die WDS-Verbindung übertragen.

SNMP-ID:

2.20.13.1.10

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

No

Nicht-VLAN-getaggte Pakete werden nicht über die WDS-Verbindung übertragen.

Yes

Nicht-VLAN-getaggte Pakete werden über die WDS-Verbindung übertragen.

Default-Wert:

Yes

Encryption

Konfigurieren Sie in dieser Tabelle alle Einstellungen rund um die Verschlüsselung und Authentisierung des Wireless Distribution Systems.

Für WDS-Verbindungen empfehlen wir, ausschließlich WPA3 zu verwenden um höchste Sicherheit zu garantieren.

SNMP-ID:

2.20.13.2

Pfad Konsole:

Setup > **WLAN** > **WDS**

Profile-Name

Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.

SNMP-ID:

2.20.13.2.1

Pfad Konsole:

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

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Method

Konfigurieren Sie hier die Verschlüsselungsmethode.

SNMP-ID:

2.20.3.2.2

Pfad Konsole:

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

Mögliche Werte:

802.11i-WPA-PSK

WPA(2/3) mit Pre-Shared-Key

WPA-Version

Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden **802.11i-WPA-PSK** und **802.11i-WPA-802.1X** verwendet werden.

SNMP-ID:

2.20.13.2.3

Pfad Konsole:

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

Mögliche Werte:

WPA1

Die WPA-Version 1 wird exklusiv verwendet.

WPA2

Die WPA-Version 2 wird exklusiv verwendet.

WPA3

Die WPA-Version 3 wird exklusiv verwendet.

WPA1/2

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 1 oder 2 verwendet.

WPA2/3

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 2 oder 3 verwendet.

WPA1-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

SNMP-ID:

2.20.13.2.4

Pfad Konsole:

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

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

WPA2-3-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 bzw. 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

SNMP-ID:

2.20.13.2.5

Pfad Konsole:

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

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

3.4.3 Max.-Distance

Geben Sie hier die Distanz zur am weitesten entfernten WLAN-Station ein (z. B. zu einem WDS-Partner).

Anhand dieser Einstellung wird der interne Timeout für WLAN-ACK-Pakete so weit erhöht, dass Pakete von einer weit entfernten Station noch verarbeitet werden können. Default ist 1 Kilometer.

SNMP-ID:

2.20.8.36

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

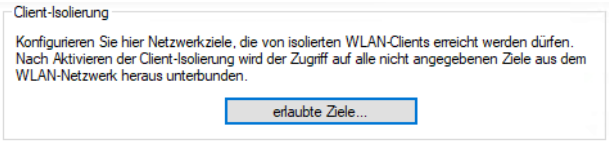
1

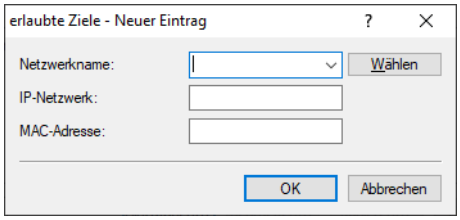
4 Client-Isolierung

Ab LCOS LX 6.10 können Sie die Kommunikation von WLAN-Clients untereinander, bzw. generell zu nicht zulässigen Zielen im Netzwerk unterbinden. Hierzu kann die Client-Isolierung konfiguriert werden.

Hierbei wird jeglicher Datenverkehr ausgehend von WLAN-Clients zu nicht explizit in einer Whitelist erfassten Zielen verboten.

Die Client-Isolierung kann je SSID eingeschaltet werden. Konfigurieren Sie dies unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** > **Client-Isolierung**. Konfigurieren Sie anschließend die erlaubten Ziele unter **Wireless-LAN** > **WLAN-Netzwerke** > **erlaubte Ziele**.





Netzwerkname

Wählen Sie hier das Netzwerk / die SSID, für die der Eintrag gelten soll. Erfassen Sie dann wahlweise eine Ziel-IP-Adresse oder Ziel-MAC-Adresse.

In Hotspot-Szenarien bietet es sich an, die MAC-Adresse des Gateways hier zu erlauben, um den Internetzugang sicherzustellen. Die Angabe dessen IP-Adresse ist nicht ausreichend, da in diesem Szenario die Ziel-IP-Adresse die eines Ziels im Internet ist.

Das Feature ermittelt die passende Gateway-Adresse automatisch aus einer DHCP-Verhandlung zwischen einem WLAN-Client und DHCP-Server. In Roaming-Szenarien wird beim Roaming allerdings üblicherweise keine erneute DHCP-Verhandlung durchgeführt, so dass in solchen Szenarien das explizite Whitelisting des Gateways erforderlich ist.

IP-Netzwerk

Erlaubte Ziel-IP-Adresse für dieses Netzwerk.

MAC-Adresse

Erlaubte Ziel-MAC-Adresse für dieses Netzwerk.

4.1 Ergänzungen im Setup-Menü

4.1.1 Client-Isolation

Soll die Kommunikation von WLAN-Clients untereinander, bzw. generell zu nicht zulässigen Zielen im Netzwerk unterbunden werden, kann die Client-Isolierung konfiguriert werden.

Hierbei wird jeglicher Datenverkehr ausgehend von WLAN-Clients zu nicht explizit in einer Whitelist erfassten Zielen verboten.

Die Client-Isolierung kann hier je SSID eingeschaltet werden. Geben Sie die erlaubten Ziele unter *2.20.5 Client-Isolation-Allowed* auf Seite 20 an.

SNMP-ID:

2.20.1.14

Pfad Konsole:

Setup > WLAN > Network

Mögliche Werte:

No

Keine Client-Isolierung.

Yes

Client-Isolierung für dieses Netzwerk aktiv.

4.1.2 Client-Isolation-Allowed

Konfigurieren Sie hier die erlaubten Ziele für die Client-Isoliserung. Siehe auch *2.20.1.14 Client-Isolation* auf Seite 20.

SNMP-ID:

2.20.5

Pfad Konsole:

Setup > WLAN

Network-Name

Wählen Sie hier das Netzwerk / die SSID, für die der Eintrag gelten soll. Erfassen Sie dann wahlweise eine Ziel-IP-Adresse (*2.20.5.2 IP-Network* auf Seite 21) oder Ziel-MAC-Adresse (*2.20.5.3 MAC-Address* auf Seite 21).

In Hotspot-Szenarien bietet es sich an, die MAC-Adresse des Gateways hier zu erlauben, um den Internetzugang sicherzustellen. Die Angabe dessen IP-Adresse ist nicht ausreichend, da in diesem Szenario die Ziel-IP-Adresse die eines Ziels im Internet ist.

Das Feature ermittelt die passende Gateway-Adresse automatisch aus einer DHCP-Verhandlung zwischen einem WLAN-Client und DHCP-Server. In Roaming-Szenarien wird beim Roaming allerdings üblicherweise keine erneute

DHCP-Verhandlung durchgeführt, so dass in solchen Szenarien das explizite Whitelisting des Gateways erforderlich ist.

SNMP-ID:

2.20.5.1

Pfad Konsole:

Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

IP-Network

Erlaubte Ziel-IP-Adresse für dieses Netzwerk.

SNMP-ID:

2.20.5.2

Pfad Konsole:

Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 19 Zeichen einer IPv4-Adresse `a.b.c.d/xx`

MAC-Address

Erlaubte Ziel-MAC-Adresse für dieses Netzwerk.

SNMP-ID:

2.20.5.3

Pfad Konsole:

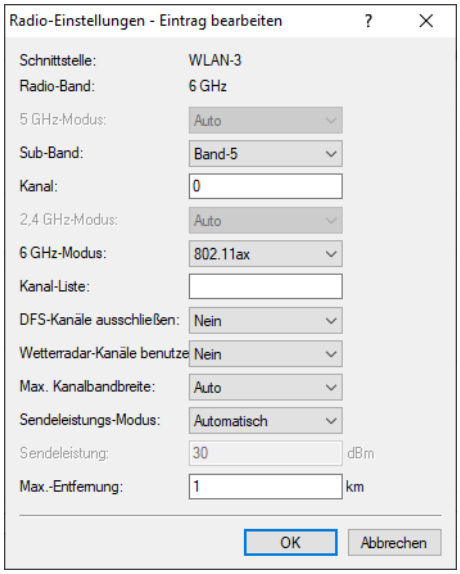
Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 17 Zeichen einer MAC-Adresse `xx:xx:xx:xx:xx:xx`

5 Wetterradar-Kanäle verwenden

Ab LCOS LX 6.10 können sie die 5 GHz-Kanäle verwenden, für die Wetterradare die Primärnutzer sind. Konfigurieren Sie in LANconfig unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** die neue Einstellung **Wetterradar-Kanäle benutzen**.



Wetterradar-Kanäle benutzen

Die von Wetterradaren verwendeten Kanäle 120, 124 und 128 im Frequenzbereich 5,6 bis 5,65 MHz werden zusätzlich von der automatischen Kanalwahl berücksichtigt und sie können explizit als Kanal angegeben werden. Wird einer der Kanäle verwendet, erhöht sich die DFS-Scan-Zeit (CAC-Time) von einer auf 10 Minuten. Während des Scans ist das 5 GHz-Radio nicht für Clients erreichbar.

5.1 Ergänzungen im Setup-Menü

5.1.1 Include-Weather-Radar-Channels

Die von Wetterradaren verwendeten Kanäle 120, 124 und 128 im Frequenzbereich 5,6 bis 5,65 MHz werden zusätzlich von der automatischen Kanalwahl berücksichtigt und sie können explizit als Kanal angegeben werden. Wird einer der Kanäle verwendet, erhöht sich die DFS-Scan-Zeit (CAC-Time) von einer auf 10 Minuten. Während des Scans ist das 5 GHz-Radio nicht für Clients erreichbar.

SNMP-ID:

2.20.8.35

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

No

Für Wetterradar reservierte Kanäle verwenden.

Yes

Für Wetterradar reservierte Kanäle nicht verwenden.

6 Layer-3-Ethernet-Tunnel mit L2TPv3

Ab LCOS LX 6.10 können Sie L2TP zum Aufbau von Ethernet-Tunneln nutzen. Die Einstellungen zur Konfiguration finden Sie im Folgenden für LANconfig, WEBconfig und CLI beschrieben.

6.1 Layer-3-Ethernet-Tunnel mit L2TPv3

LCOS LX unterstützt das Layer 2 Tunneling Protocol (L2TP) in Version 3. Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Datentypen

L2TP verwendet zwei Typen von Daten:

Steuerdaten

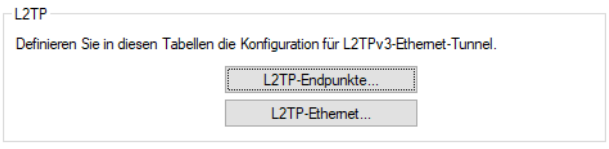
Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

Nutzdaten

Die Nutzdaten kapseln die Ethernet-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

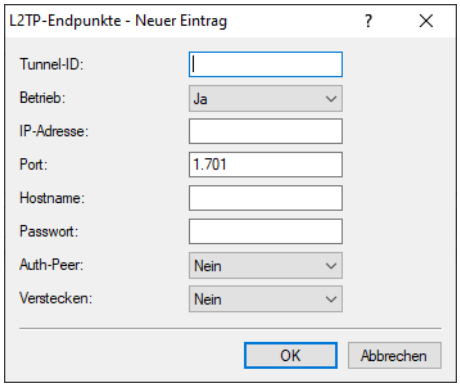
Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

LANconfig: **Sonstige Dienste** > **L2TP**



6.1.1 L2TP-Endpunkte

Über **L2TP-Endpunkte** konfigurieren Sie die L2TP-Endpunkte für die L2TPv3-Tunnel. Damit nehmen Sie die Tunnel-Konfiguration für die Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt vor.



Tunnel-ID

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Betrieb

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts.

Port

Der zu nutzende UDP-Port. Default: 1701

Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Passwort

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

Verstecken

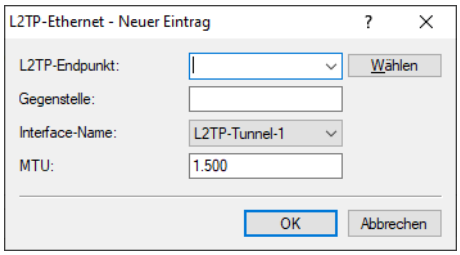
Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

Verbinden Sie anschließend ein konfiguriertes WLAN-Netzwerk mit der virtuellen L2TP-Ethernet-Schnittstelle.

Wechseln Sie dazu zu **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** und setzen Sie im gewünschten Eintrag die Einstellung **Bridge** auf die soeben konfigurierte virtuelle L2TP-Ethernet-Schnittstelle.

6.1.2 L2TP-Ethernet

Über **L2TP-Ethernet** konfigurieren Sie den L2TPv3-Tunnel zwischen einem WLAN-Netzwerk und einem L2TP-Endpunkt.



L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut.

Gegenstelle

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

Interface-Name

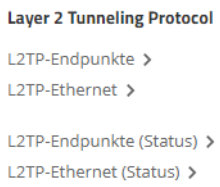
Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

MTU

Diese Einstellung passt die MTU eines L2TP-Ethernet-Tunnels auf den angegebenen Wert an, z. B. bei Verbindung des Tunnels über Netzwerke mit kleinerer MTU hinweg. Mögliche Werte: 68-1500

6.2 Layer-3-Ethernet-Tunnel mit L2TPv3

Die Einstellungen für das Layer-3-Ethernet-Tunnel mit L2TPv3 finden Sie in der WEBconfig unter **Systemkonfiguration** > **Layer 2 Tunneling Protocol**.



LCOS LX unterstützt das Layer 2 Tunneling Protocol (L2TP) in Version 3. Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Datentypen

L2TP verwendet zwei Typen von Daten:

Steuerdaten

Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

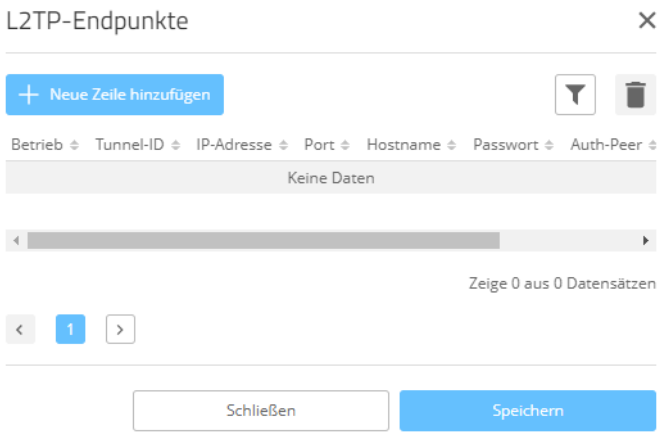
Nutzdaten

Die Nutzdaten kapseln die Ethernet-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

6.2.1 L2TP-Endpunkte

Über **L2TP-Endpunkte** konfigurieren Sie die L2TP-Endpunkte für die L2TPv3-Tunnel. Damit nehmen Sie die Tunnel-Konfiguration für die Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt vor.



Tunnel-ID

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Betrieb

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts.

Port

Der zu nutzende UDP-Port. Default: 1701

Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Passwort

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

Auth-Peer

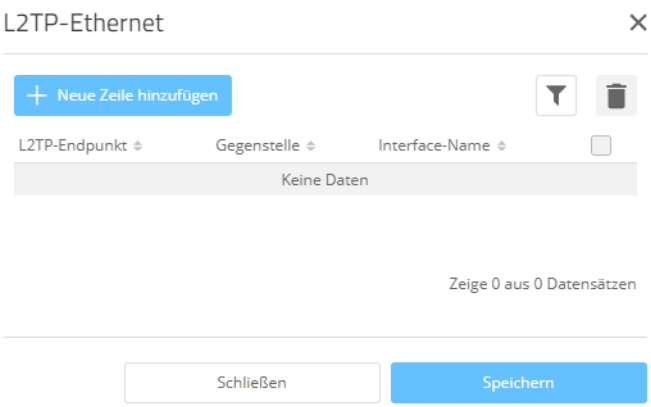
Angabe, ob die Gegenstelle authentifiziert werden soll.

Verstecken

Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

6.2.2 L2TP-Ethernet

Über **L2TP-Ethernet** konfigurieren Sie den L2TPv3-Tunnel zwischen einem WLAN-Netzwerk und einem L2TP-Endpunkt.



L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut.

Gegenstelle

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

Interface-Name

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

MTU

Diese Einstellung passt die MTU eines L2TP-Ethernet-Tunnels auf den angegebenen Wert an, z. B. bei Verbindung des Tunnels über Netzwerke mit kleinerer MTU hinweg. Mögliche Werte: 68-1500

6.2.3 L2TP-Status

Unter **L2TP-Endpunkte (Status)** und **L2TP-Ethernet (Status)** werden Ihnen Statusinformationen zu den L2TP-Tunneln angezeigt.

6.3 Ergänzungen im Setup-Menü

6.3.1 L2TP

LCOS LX unterstützt das Layer 2 Tunneling Protocol (L2TP) in Version 3. Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Datentypen

L2TP verwendet zwei Typen von Daten:

Steuerdaten

Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

Nutzdaten

Die Nutzdaten kapseln die Ethernet-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

SNMP-ID:

2.61

Pfad Konsole:

Setup

Endpoints

In dieser Tabelle werden die grundsätzlichen Einstellungen zur Konfiguration eines L2TP-Tunnels vorgenommen.

Sollen RAS-Verbindungen ohne Konfiguration in einem Gerät über RADIUS authentifiziert werden, muss in dieser Tabelle ein Default-Eintrag mit folgenden Werten angelegt werden:

- **Tunnel-Id**: DEFAULT
- **Auth-Peer**: Yes
- **Hide**: No

Alle anderen Werte müssen leer bleiben. Wird **Auth-Peer** im DEFAULT-Eintrag auf „No“ gesetzt, werden alle Hosts ungeprüft angenommen und nur die PPP-Sessions authentifiziert.

SNMP-ID:

2.61.1

Pfad Konsole:

Setup > **L2TP**

Tunnel-Id

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

SNMP-ID:

2.61.1.1

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

IP-Address

Die IP-Adresse des Tunnel-Endpunkts. Anstelle einer IP-Adresse (IPv4 oder IPv6) kann auch ein FQDN angegeben werden.

SNMP-ID:

2.61.1.2

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Port

Der zu nutzende UDP-Port.

SNMP-ID:

2.61.1.3

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

0 … 65535

Default-Wert:

1701

Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

SNMP-ID:

2.61.1.4

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

Password

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

SNMP-ID:

2.61.1.5

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

SNMP-ID:

2.61.1.6

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

No

Gegenstelle muss nicht authentifiziert werden.

Yes

Gegenstelle muss authentifiziert werden.

Default-Wert:

No

Hide

Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

SNMP-ID:

2.61.1.7

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

No

Tunnelaushandlung wird nicht verschleiert.

Yes

Tunnelaushandlung wird verschleiert.

Default-Wert:

No

Operating

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

SNMP-ID:

2.61.1.8

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

Nein

L2TP-Endpunkt ist inaktiv.

Ja

L2TP-Endpunkt ist aktiv.

Default-Wert:

Ja

Ethernet

In dieser Tabelle verknüpfen Sie L2TPv3-Endpunkte mit einem WLAN-Netzwerk.

SNMP-ID:

2.61.2

Pfad Konsole:

Setup > **L2TP**

L2TP-Endpoint

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts (*2.61.1.1 Tunnel-Id* auf Seite 30). Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen". Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.

SNMP-ID:

2.61.2.1

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

Remote-End

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

SNMP-ID:

2.61.2.2

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

Interface-Name

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

SNMP-ID:

2.61.2.3

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtuelle L2TP-Ethernet-Schnittstellen

MTU

Diese Einstellung passt die MTU eines L2TP-Ethernet-Tunnels auf den angegebenen Wert an, z. B. bei Verbindung des Tunnels über Netzwerke mit kleinerer MTU hinweg.

SNMP-ID:

2.61.2.4

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

68 … 1500

Default-Wert:

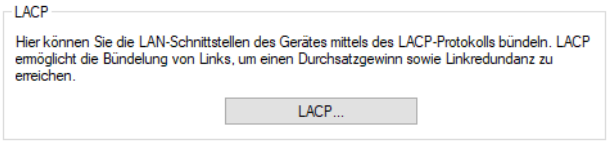
1500

7 Link Aggregation (LACP)

Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von LAN-Ports zu einem virtuellen Link. Physikalische Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

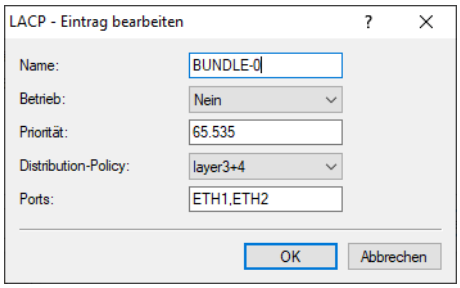
Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

LANconfig: **Sonstige Dienste** > **Link Aggregation**



7.1 LACP (Link Aggregation Control Protocol)

Über **LACP** konfigurieren Sie das Link Aggregation Control Protocol.



Name

Die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

Betrieb

Über diesen Parameter aktivieren oder deaktivieren Sie die Schnittstellen-Bündelung.

Wenn Sie die Bündelung aktivieren, fasst das Gerät die gewählten Geräte-Schnittstellen unter einer gemeinsamen logischen Bündel-Schnittstelle zusammen. Im deaktivierten Zustand bleiben die in der dazugehörigen Tabelle ausgewählten Schnittstellen als eigenständige Schnittstellen nutzbar.

Priorität

Tragen Sie hier die LACP-System-Priorität ein. Der Standardwert ist 65.535.

Distribution-Policy

Zur Verteilung der Netzwerkpakete auf die verschiedenen gebündelten Schnittstellen steht eine Vielzahl von Möglichkeiten bereit. Folgende Merkmale werden jeweils zur Verteilung herangezogen:

layer2

MAC-Adressen

layer2+3

Eine Kombination aus MAC-Adressen und IP-Adressen

layer3+4

IP-Adressen und TCP/UDP-Ports

encap2+3

Wie layer2+3. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

encap3+4

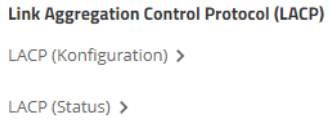
Wie layer3+4. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt. Default: ETH1,ETH2

7.2 Link Aggregation Control Protocol (LACP)

Die Einstellungen für das Link Aggregation Control Protocol (LACP) finden Sie in der WEBconfig unter **Systemkonfiguration** > **Link Aggregation Control Protocol (LACP)**.



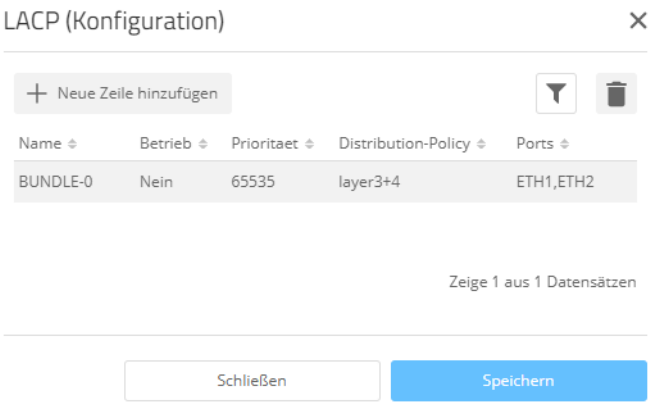
Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von LAN-Ports zu einem virtuellen Link. Physikalische Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

LANconfig: **Sonstige Dienste** > **Link Aggregation**

7.2.1 LACP (Konfiguration)

Über **LACP** konfigurieren Sie das Link Aggregation Control Protocol.



Name

Die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

Betrieb

Über diesen Parameter aktivieren oder deaktivieren Sie die Schnittstellen-Bündelung.

Wenn Sie die Bündelung aktivieren, fasst das Gerät die gewählten Geräte-Schnittstellen unter einer gemeinsamen logischen Bündel-Schnittstelle zusammen. Im deaktivierten Zustand bleiben die in der dazugehörigen Tabelle ausgewählten Schnittstellen als eigenständige Schnittstellen nutzbar.

Priorität

Tragen Sie hier die LACP-System-Priorität ein. Der Standardwert ist 65.535.

Distribution-Policy

Zur Verteilung der Netzwerkpakete auf die verschiedenen gebündelten Schnittstellen steht eine Vielzahl von Möglichkeiten bereit. Folgende Merkmale werden jeweils zur Verteilung herangezogen:

layer2

MAC-Adressen

layer2+3

Eine Kombination aus MAC-Adressen und IP-Adressen

layer3+4

IP-Adressen und TCP/UDP-Ports

encap2+3

Wie layer2+3. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

encap3+4

Wie layer3+4. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt. Default: ETH1,ETH2

7.2.2 LACP (Status)

Unter **LACP (Status)** werden Ihnen Statusinformationen zu den LACP-Verbindungen angezeigt.

7.3 Ergänzungen im Setup-Menü

7.3.1 LAN

Hier finden Sie die Einstellungen, welche die LAN-Anbindung des Access Points betreffen.

SNMP-ID:

2.62

Pfad Konsole:

Setup

LACP

Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von LAN-Ports zu einem virtuellen Link. Physikalische Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

SNMP-ID:

2.62.1

Pfad Konsole:

Setup > **LAN**

Name

Dieser Parameter zeigt die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

SNMP-ID:

2.62.1.1

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

max. 9 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

BUNDLE-0

Operating

Über diesen Parameter aktivieren oder deaktivieren Sie die Schnittstellen-Bündelung.

Wenn Sie die Bündelung aktivieren, fasst das Gerät die gewählten Geräte-Schnittstellen unter einer gemeinsamen logischen Bündel-Schnittstelle zusammen. Im deaktivierten Zustand bleiben die in der dazugehörigen Tabelle ausgewählten Schnittstellen als eigenständige Schnittstellen nutzbar.

SNMP-ID:

2.62.1.2

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

No
Yes

Priority

Tragen Sie hier die LACP-System-Priorität ein.

SNMP-ID:

2.62.1.3

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

Vielfache von 4096 `max. 6 Zeichen aus[0-9]`

Default-Wert:

65535

Distribution-Policy

Zur Verteilung der Netzwerkpakete auf die verschiedenen gebündelten Schnittstellen steht eine Vielzahl von Möglichkeiten bereit. Folgende Merkmale werden jeweils zur Verteilung herangezogen:

layer2

MAC-Adressen

layer2+3

Eine Kombination aus MAC-Adressen und IP-Adressen

layer3+4

IP-Adressen und TCP/UDP-Ports

encap2+3

Wie layer2+3. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

encap3+4

Wie layer3+4. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

SNMP-ID:

2.62.1.4

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

layer2
layer2+3
layer3+4
encap2+3
encap3+4

Default-Wert:

layer3+4

Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt.

SNMP-ID:

2.62.1.5

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

max. 16 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

ETH1,ETH2