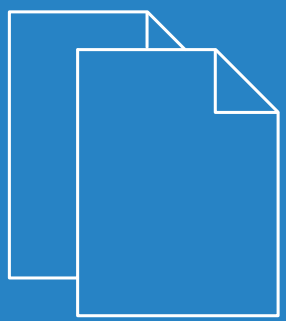
SICHER. **VERNETZT.**

LCOS LX 5.10

Addendum



02/2020

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS LX-Version 5.10

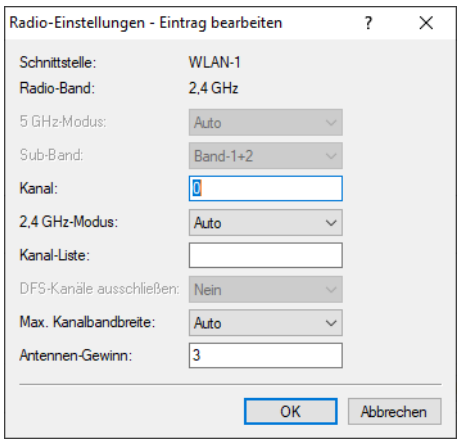
Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 5.10 gegenüber der vorherigen Version.

2 Wi-Fi 6

WLAN ist heutzutage allgegenwärtig – die Nutzeranzahl steigt wie die Anwendungsmöglichkeiten rasant. Wi-Fi 6 ermöglicht hierfür nicht ausschließlich mehr Tempo, sondern vor allem eine echte Steigerung des durchschnittlichen Durchsatzes pro WLAN-Client. Dank einem effizienteren Umgang mit den knappen Bändern und Kanälen, die zur Verfügung stehen, bringt Wi-Fi 6 mehr Stabilität und Zuverlässigkeit in hoch beanspruchten WLANs.

LCOS LX Access Points mit entsprechender Hardware für Wi-Fi 6 wie z. B. ein LANCOM LX-6400 unterstützen diesen Standard ohne weitere Einstellungen.

In LANconfig konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** alle Einstellungen rund um die physikalischen Radio-Parameter. Standardmäßig ist für jedes physikalisch vorhandene WLAN-Radio ein Eintrag in der Tabelle enthalten, der bei Bedarf modifiziert werden kann. Für Wi-Fi 6 sind die folgenden Optionen zuständig:



5 GHz-Modus

Konfigurieren Sie hier, in welchem Modus das 5-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

11an-mixed

Es werden die Modi 802.11a und 802.11n verwendet.

11anac-mixed

Es werden die Modi 802.11a, 802.11n und 802.11ac verwendet.

11nac-mixed

Es werden die Modi 802.11n und 802.11ac verwendet.

11ac-only

Es wird nur der Modus 802.11ac verwendet.

11anacax-mixed

Es werden die Modi 802.11a, 802.11n, 802.11ac und 802.11ax (Wi-Fi 6) verwendet.

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

2,4 GHz-Modus

Konfigurieren Sie hier, in welchem Modus das 2,4-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

11bg-mixed

Es werden die Modi 802.11b und 802.11g verwendet.

11g-only

Es wird nur der Modus 802.11g verwendet.

11bgn-mixed

Es werden die Modi 802.11b, 802.11g und 802.11n verwendet.

11gn-mixed

Es werden die Modi 802.11g und 802.11n verwendet.

11bgnax-mixed

Es werden die Modi 802.11b, 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

11gnax-mixed

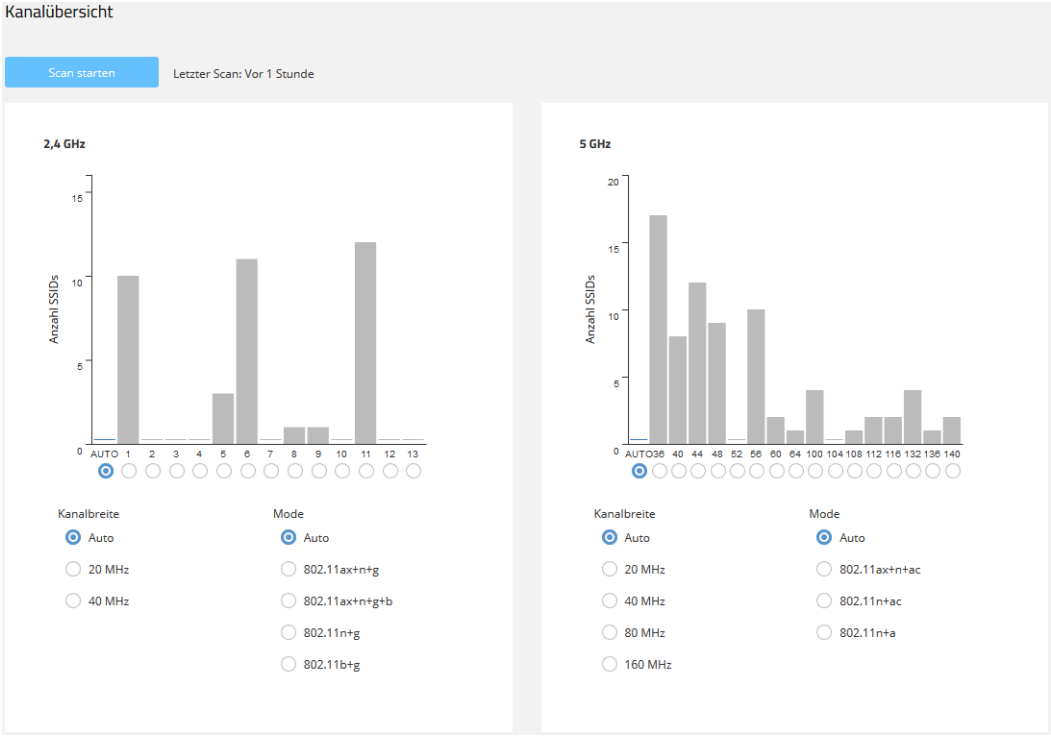
Es werden die Modi 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

In WEBconfig ist dies über die Einstellungen im Bereich **Technologie** bei der jeweiligen SSID in der **WLAN-Konfiguration** möglich:

Die Seite **Technologie** bietet die Möglichkeit, feste Kanäle für das 2,4- und 5-GHz-Band festzulegen, sowohl die verwendete Kanalbreite und den verwendeten Radio-Modus zu bestimmen. Voreingestellt ist für alle Möglichkeiten die automatische Auswahl. Weiter unten auf der Seite finden Sie die Einstellungen zum Client-Management.

Die hier konfigurierbaren physikalischen Einstellungen gelten für das gesamte jeweilige Frequenzband und sind nicht SSID-spezifisch.



Die beiden Balkendiagramme visualisieren, wie viele SSIDs vom Gerät auf den verschiedenen 2,4- und 5-GHz-Kanälen erkannt wurden und potentiell eine Belastung des Mediums auf diesem Kanal darstellen.

Die Balkendiagramme werden nur mit Informationen befüllt, wenn zuvor entweder hier oder im Bereich **Nachbarschaft** ein Nachbarschaftsscan durchgeführt wurde.

2.1 Ergänzungen im Setup-Menü

2.1.1 5GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 5-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

SNMP-ID:

2.20.8.3

Pfad Konsole:

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

Mögliche Werte:

11an-mixed
Es werden die Modi 802.11a und 802.11n verwendet.

11anac-mixed
Es werden die Modi 802.11a, 802.11n und 802.11ac verwendet.

11nac-mixed
Es werden die Modi 802.11n und 802.11ac verwendet.

11ac-only
Es wird nur der Modus 802.11ac verwendet.

11anacax-mixed
Es werden die Modi 802.11a, 802.11n, 802.11ac und 802.11ax (Wi-Fi 6) verwendet.

Auto
Es werden alle vom Gerät unterstützten Modi verwendet.

2.1.2 2.4GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 2,4-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt.

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

SNMP-ID:

2.20.8.9

Pfad Konsole:

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

Mögliche Werte:

11bg-mixed
Es werden die Modi 802.11b und 802.11g verwendet.

11g-only
Es wird nur der Modus 802.11g verwendet.

11bgn-mixed
Es werden die Modi 802.11b, 802.11g und 802.11n verwendet.

11gn-mixed
Es werden die Modi 802.11g und 802.11n verwendet.

11bgnax-mixed
Es werden die Modi 802.11b, 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

11gnax-mixed
Es werden die Modi 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

Auto
Es werden alle vom Gerät unterstützten Modi verwendet.

3 Schnelles WLAN-Roaming

Fast Roaming, nach dem WLAN-Standard IEEE 802.11r, ermöglicht schnelle Roaming-Vorgänge von Clients zwischen Access Points für ein optimales WLAN-Nutzungserlebnis.

Zusammen mit der Authentifizierung nach dem Standard IEEE 802.1X und dem Schlüsselmanagement nach dem Standard IEEE 802.11i bieten moderne WLAN-Installationen ein hohes Maß an Sicherheit und Vertraulichkeit der übertragenen Daten. Allerdings erfordern diese Standards die Übertragung zusätzlicher Datenpakete während der Verbindungsverhandlung sowie zusätzliche Rechenleistung auf Client- und Serverseite.

IEEE 802.11 benötigte ursprünglich zum Aufbau einer Datenverbindung zwischen WLAN-Client und Accesss Point lediglich bis zu sechs Datenpakete. Die Standard-Erweiterung IEEE 802.11i besserte Schwachstellen bei der WEP-Verschlüsselung aus, verlängerte dabei jedoch den Anmeldeprozess je nach Authentifizierungsmethode um ein Vielfaches.

Diese verlängerte Anmeldezeit des WLAN-Clients am Accesss Point ist für nicht zeitkritische Anwendungen ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem Accesss Point zum nächsten, ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel. Als Beispiel seien hier Voice-over-IP (VoIP) oder die Anwendung in industriellen Echtzeit-Umgebungen genannt. Roaming bedeutet in diesem Zusammenhang, dass die Netzwerkverbindung ohne Abbruch von einem Access Point auf den anderen übergeht.

Methoden wie Pairwise Master Key Caching (PMK Caching), Pre-Authentication, Opportunistic Key Caching (OKC) sowie der Einsatz von zentralen WLAN-Controllern (WLC) zur Schlüsselverwaltung verbessern die Zeit für die Schlüsselaushandlung zwischen WLAN-Client und Accesss Point bei der Anmeldung. Allerdings reicht das immer noch nicht aus, die vergleichsweise lange Zeit für die Schlüsselverhandlung zwischen WLAN-Client und Accesss Point auf ein brauchbares Maß zu begrenzen.

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim Accesss Point zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim Accesss Point. Beim Roaming von einem Accesss Point zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen Accesss Point reservieren. Die dafür notwendigen zusätzlichen Management-Frames erhöhen die Anmeldezeit jedoch wieder deutlich.

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem Accesss Point zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am Access Point wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Wie beim Opportunistic Key Caching (OKC) existiert eine zentrale Schlüssel-Verwaltung, sinnvollerweise in Form eines WLCs, der die angeschlossenen Accesss Points mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der Accesss Point IEEE 802.11r beherrscht.

Die vom WLC verwalteten Accesss Points senden als Kennung das sogenannte „Mobility Domain Information Element (MDIE)“ aus, das den WLAN-Clients im Empfangsbereich u. a. mitteilt, welcher „Mobility Group“ der Accesss Point angehört. Anhand dieser Gruppenkennung erkennt der WLAN-Client, ob er derselben Domain angehört und sich somit ohne Verzögerung anmelden kann. Diese Mobility Domain hat der WLAN-Client während der ersten Anmeldung an einem Accesss Point mitgeteilt bekommen.

Die Domain-Kennung sowie spezielle, bei der Erstanmeldung generierte und an alle verwalteten Accesss Points übertragenen Schlüssel verringern die Verhandlungsschritte bei der Neuanmeldung bei einem Accesss Point auf die angestrebten vier bis sechs Schritte.

Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen Accesss Point einen neuen PMK aushandeln. Dieser ist auch auf dem Accesss Point gültig, mit dem sich der WLAN-Client im Anschluss verbinden möchte.

Zusätzlich ermöglicht IEEE 802.11r in Form eines „Resource Requests" die Reservierung von zusätzlicher Bandbreite auf dem neuen Accesss Point, ohne dass weitere Datenpakete wie bei IEEE 802.11e die Anmeldung unnötig verlängern.

Ältere WLAN-Clients haben möglicherweise Probleme damit, eine Verbindung zu einer SSID mit aktiviertem 802.11r aufzubauen. Daher ist hier der Einsatz zweier SSIDs ratsam: eine SSID für ältere Clients ohne 802.11r-Unterstützung und eine weitere SSID mit aktiviertem 802.11r für Clients mit 802.11r-Unterstützung.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Fast Roaming über Inter Access Point Protocol (IAPP)

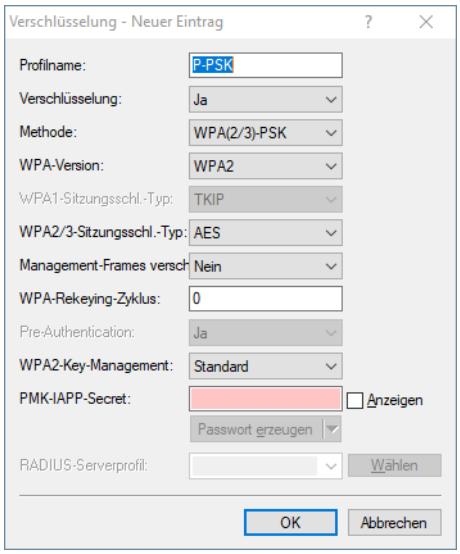
Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Beim Wechsel eines Clients zu einem anderen Access Point informiert (Handover Request) der übernehmende Access Point den ehemals bedienenden Access Point. Der ehemalige Access Point löscht daraufhin den Client aus seiner Stationstabelle. Im Handover Request ist die MAC-Adresse des Clients enthalten, sodasss im LAN vorhandene Geräte über das neue Routing informiert werden und ihre Zuordnungstabelle aktualisieren können.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **Wireless-LAN** > **Allgemein** > **Verschlüsselung** > **PMK-IAPP-Secret**.

Beachten Sie bitte, dass es für die Verwendung von Fast Roaming über IAPP erforderlich ist, in den Verschlüsselungs-Einstellungen unter WPA2-Key-Management die Option Fast Roaming auszuwählen.

Fast Roaming konfigurieren

In LANconfig konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke.



WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll. Mögliche Werte:

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Standard+Fast-Roaming

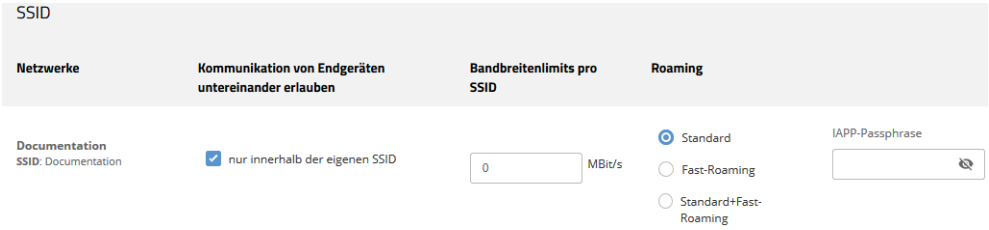
Kombination aus Standard und Fast Roaming

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am Access Point anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als Standard aktiviert ist.

PMK-IAPP-Secret

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Stellen Sie daher sicher, dass diese Passphrase auf allen Access Points, zwischen denen mittels Fast Roaming geroamt werden soll, identisch ist.

In WEBconfig ist dies über die Einstellungen im Bereich **SSID** in der **WLAN-Konfiguration** möglich:



Roaming

Einstellungen zum Wechsel eines Clients von einem Access Point zu einem anderen Access Point, der die gleiche SSID ausstrahlt.

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Prä-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Standard+Fast-Roaming

Eine Kombination aus dem Standardverhalten und Fast Roaming.

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am Access Point anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als Standard aktiviert ist.

IAPP-Passphrase

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Stellen Sie daher sicher, dass diese Passphrase auf allen Access Points, zwischen denen mittels Fast Roaming geroamt werden soll, identisch ist.

3.1 Ergänzungen im Setup-Menü

3.1.1 WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll.

SNMP-ID:

2.20.3.19

Pfad Konsole:

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

Mögliche Werte:

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r.

Standard+Fast-Roaming

Kombination aus Standard und Fast Roaming

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am Access Point anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als Standard aktiviert ist.

3.1.2 PMK-IAPP-Secret

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Stellen Sie daher sicher, dass diese Passphrase auf allen Access Points, zwischen denen mittels Fast Roaming geroamt werden soll, identisch ist.

SNMP-ID:

2.20.3.20

Pfad Konsole:

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

Mögliche Werte:

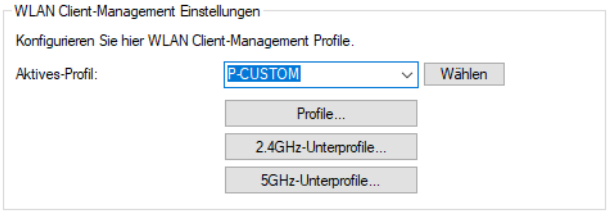
max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

4 Band Steering – Volle Bandbreite durch intelligente Client-Steuerung!

Band Steering ermöglicht eine optimale Lastverteilung im WLAN durch eine aktive Steuerung von Clients auf das weniger ausgelastete und leistungsstärkere 5-GHz-Frequenzband. Je nach den Fähigkeiten des WLAN-Clients wird dieser hierbei durch den Access Point auf das präferierte Frequenzband geleitet – nahezu unterbrechungsfrei mittels des modernen Verfahrens 802.11v.

4.1 Client Management

Die Einstellungen zum Band Steering für WLAN-Netzwerke finden Sie unter **Wireless-LAN** > **Client-Management**.



Aktives Profil

Wählen Sie hier das Profil, welches die Einstellungen für das Band-Steering-Modul festlegt.

P-DEFAULT

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz auf dem aktuellen Kanal und erfolgt bevorzugt mittels 802.11v. Unterstützt der Client kein 802.11v, wird das Steering mittels einer gezielten Disassoziierung des Clients durchgeführt. Das Steering erfolgt sowohl vor der Assoziierung, als auch, bei Bedarf, während der Client bereits assoziiert ist. Dies ist das empfohlene Profil.

P-DISABLED

Es wird keinerlei Steering durchgeführt. Der Client entscheidet autark, welches Frequenzband er wählt.

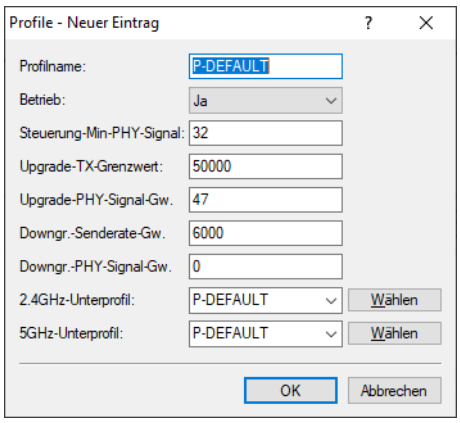
P-LEGACY

Steering erfolgt vor der Assoziierung des Clients durch gezielte Zurückhaltung von Probe Responses. Es wird unabhängig von der Auslastung immer das 5-GHz-Band bevorzugt.

4.1.1 Profile

Passen Sie unter **Wireless-LAN** > **Client-Management** > **Profile** die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

LANCOM empfiehlt die Verwendung der voreingestellten Profile.



Profilname

Geben Sie diesem Profil einen Namen.

Betrieb

Steuert, ob das Band Steering für dieses Profil aktiv ist.

Steuerung-Min-PHY-Signal

Legt die Client-Signalstärke (in dB) fest, ab der ein Steering des Clients durchgeführt wird.

Upgrade-TX-Grenzwert

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen erreichen potentiell ein Steering des Clients auf das 5-GHz-Band erfolgen soll.

Upgrade-PHY-Signal-Grenzwert

Legt die Client-Signalstärke (in dB) fest, die mindestens erreicht sein muss, damit der Client für ein Steering auf das 5-GHz-Band in Betracht gezogen wird.

Downgrade-Senderate-Grenzwert

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen Erreichen potentiell ein Steering des Clients auf das 2,4-GHz-Band erfolgen soll.

Downgrade-PHY-Signal-Grenzwert

Legt die Client-Signalstärke (in dB) fest, die unterschritten sein muss, damit der Client für ein Steering auf das 2,4-GHz-Band in Betracht gezogen wird.

Für ein Steering auf 2,4 GHz (Downgrade) muss sowohl die hier konfigurierte Signalstärke unterschritten sein, als auch der Grenzwert aus **Abwertung-Senderate-Grenzwert** erreicht werden.

2,4-GHz-Unterprofil

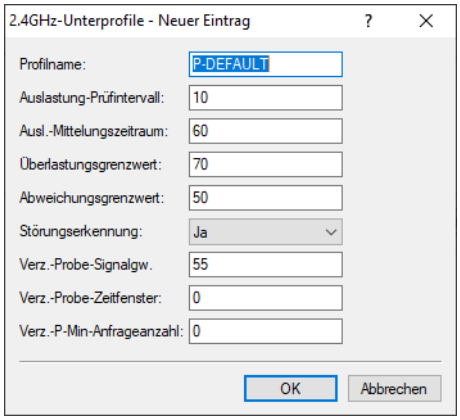
Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

5-GHz-Unterprofil

Konfigurieren Sie hier, welches 5-GHz-Unterprofil zur Anwendung kommt.

4.1.2 2,4-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **2,4 GHz-Unterprofile** die Einstellungen der 2,4-GHz-Unterprofile.



Profilname

Geben Sie diesem 2,4-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Auslastung-Mitteilungszeitraum

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das **Auslastung-Prüfintervall** konfiguriertem Wert liegen.

Überlastungsgrenzwert

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 2,4-GHz-Kanal als ausgelastet angenommen wird.

Abweichungsgrenzwert

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Störungserkennung

Konfiguriert, ob Interferenzen auf dem konfigurierten 2,4-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

Verzögerung Probe-Signalgrenzwert

Legt die Client-Signalstärke (in dB) fest, die erreicht sein muss, damit Probe Responses an den Client zum Zwecke des Steerings zurückgehalten werden.

Verzögerung Probe-Zeitfenster

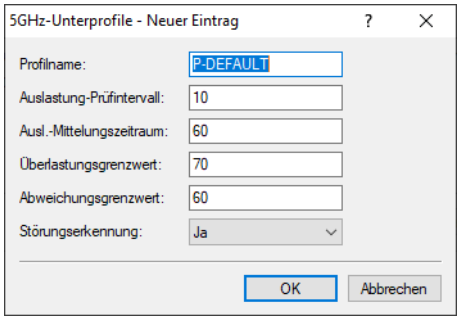
Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Verzögerung Probe-Min.-Anfrageanzahl** konfiguriert wurde, damit diese beantwortet werden.

Verzögerung Probe-Min.-Anfrageanzahl

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Verzögerung Probe Zeitfenster** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

4.1.3 5-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **5 GHz-Unterprofile** die Einstellungen der 5-GHz-Unterprofile.



Profilname

Geben Sie diesem 5-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Auslastung-Mitteilungszeitraum

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das **Auslastung-Prüfintervall** konfiguriertem Wert liegen.

Überlastungsgrenzwert

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 5-GHz-Kanal als ausgelastet angenommen wird.

Abweichungsgrenzwert

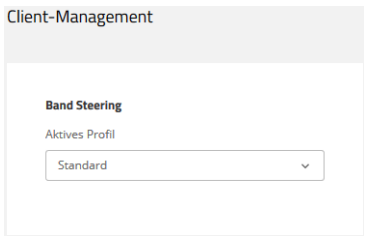
Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Störungserkennung

Konfiguriert, ob Interferenzen auf dem konfigurierten 5-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

4.2 Client Management über WEBconfig einstellen

In WEBconfig ist dies über die Einstellungen im Bereich **Technologie** bei der jeweiligen SSID in der **WLAN-Konfiguration** möglich:



Aktives Profil

Wählen Sie hier das Profil, welches die Einstellungen für das Band-Steering-Modul festlegt.

Standard

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz auf dem aktuellen Kanal und erfolgt bevorzugt mittels 802.11v. Unterstützt der Client kein 802.11v, wird das Steering mittels einer gezielten Disassoziierung des Clients durchgeführt. Das Steering erfolgt sowohl vor der Assoziierung, als auch, bei Bedarf, während der Client bereits assoziiert ist. Dies ist das empfohlene Profil.

Ausgeschaltet

Es wird keinerlei Steering durchgeführt. Der Client entscheidet autark, welches Frequenzband er wählt.

Legacy

Steering erfolgt vor der Assoziierung des Clients durch gezielte Zurückhaltung von Probe Responses. Es wird unabhängig von der Auslastung immer das 5-GHz-Band bevorzugt.

4.3 Ergänzungen im Setup-Menü

4.3.1 Client-Management

Konfigurieren Sie hier die Einstellungen zum Band Steering. Mittels Band Steering können Clients vom überlaufenen 2,4-GHz-Frequenzband auf das 5-GHz-Frequenzband gelenkt werden, sodass für den einzelnen Client mehr Bandbreite zur Verfügung steht und die Benutzererfahrung verbessert wird. LCOS LX bietet die Möglichkeit, Clients mittels des 802.11v-Standards auf das jeweils für sie optimale Frequenzband zu leiten. Auch Clients, die den 802.11v-Standard nicht unterstützen, können durch eine gezielte Verzögerung von Probe Responses oder gezielte Trennung vom WLAN auf das 5-GHz-Band geleitet werden.

SNMP-ID:

2.20.4

Pfad Konsole:

Setup > **WLAN**

Active-Profile

Wählen Sie hier das Profil, welches die Einstellungen für das Band-Steering-Modul festlegt.

SNMP-ID:

2.20.4.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

Mögliche Werte:

P-DEFAULT

Steering erfolgt anhand der Mediumsauslastung und der erkannten Intereferenz auf dem aktuellen Kanal und erfolgt bevorzugt mittels 802.11v. Unterstützt der Client kein 802.11v, wird das Steering mittels einer gezielten Disassoziierung des Clients durchgeführt. Das Steering erfolgt sowohl vor der Assoziierung, als auch, bei Bedarf, während der Client bereits assoziiert ist. Dies ist das empfohlene Profil.

P-LEGACY

Steering erfolgt vor der Assoziierung des Clients durch gezielte Zurückhaltung von Probe Responses. Es wird unabhängig von der Auslastung immer das 5-GHz-Band bevorzugt.

P-DISABLED

Es wird keinerlei Steering durchgeführt. Der Client entscheidet autark, welches Frequenzband er wählt.

<Custom>

Neben den vorgegebenen Profilen können Sie auch in **Profiles** selbst erstellte Profile einstellen.

Default-Wert:

P-DEFAULT

Profiles

Passen Sie hier die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

SNMP-ID:

2.20.4.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

Profile-Name

Der Name des Profils.

SNMP-ID:

2.20.4.2.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

Operating

Steuert, ob das Band Steering für dieses Profil aktiv ist.

SNMP-ID:

2.20.4.2.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No

Band Steering ist nicht aktiv.

Yes

Band Steering ist aktiv.

Steering-Min-PHY-Signal

Legt die Client-Signalstärke (in dB) fest, ab der ein Steering des Clients durchgeführt wird.

SNMP-ID:

2.20.4.2.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Upgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen erreichen potentiell ein Steering des Clients auf das 5-GHz-Band erfolgen soll.

SNMP-ID:

2.20.4.2.4

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Upgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die mindestens erreicht sein muss, damit der Client für ein Steering auf das 5-GHz-Band in Betracht gezogen wird.

SNMP-ID:

2.20.4.2.5

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Downgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen Erreichen potentiell ein Steering des Clients auf das 2,4-GHz-Band erfolgen soll.

SNMP-ID:

2.20.4.2.6

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Downgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die unterschritten sein muss, damit der Client für ein Steering auf das 2,4-GHz-Band in Betracht gezogen wird.

Für ein Steering auf 2,4 GHz (Downgrade) muss sowohl die hier konfigurierte Signalstärke unterschritten sein, als auch der Grenzwert aus **Downgrade-TX-Rate-Threshold** erreicht werden.

SNMP-ID:

2.20.4.2.7

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.4GHz-Sub-Profile

Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

SNMP-ID:

2.20.4.2.8

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

5GHz-Sub-Profile

Konfigurieren Sie hier, welches 5-GHz-Unterprofil zur Anwendung kommt.

SNMP-ID:

2.20.4.2.9

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.4GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 2,4-GHz-Unterprofile.

SNMP-ID:

2.20.4.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

Profile-Name

Der Profilname des 2,4-GHz-Unterprofils.

SNMP-ID:

2.20.4.3.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

SNMP-ID:

2.20.4.3.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

SNMP-ID:

2.20.4.3.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 2,4-GHz-Kanal als ausgelastet angenommen wird.

SNMP-ID:

2.20.4.3.4

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

SNMP-ID:

2.20.4.3.5

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 2,4-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

SNMP-ID:

2.20.4.3.6

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

Delay-Probe-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die erreicht sein muss, damit Probe Responses an den Client zum Zwecke des Steerings zurückgehalten werden.

SNMP-ID:

2.20.4.3.7

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Delay-Probe-Time-Window

Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Delay-Probe-Min-Request-Count** konfiguriert wurde, damit diese beantwortet werden.

SNMP-ID:

2.20.4.3.8

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Delay-Probe-Min-Request-Count

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Delay-Probe-Time-Window** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

SNMP-ID:

2.20.4.3.9

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

5GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 5-GHz-Unterprofile.

SNMP-ID:

2.20.4.4

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

Profile-Name

Der Profilname des 5-GHz-Unterprofils.

SNMP-ID:

2.20.4.4.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

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

Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

SNMP-ID:

2.20.4.4.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

SNMP-ID:

2.20.4.4.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 5-GHz-Kanal als ausgelastet angenommen wird.

SNMP-ID:

2.20.4.4.4

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

SNMP-ID:

2.20.4.4.5

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 5-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

SNMP-ID:

2.20.4.4.6

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

5 LANCOM Enhanced Passphrase Security User (LEPS-U)

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) kann eine Menge von Passphrasen konfiguriert werden, die dann den einzelnen Benutzern oder Gruppen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

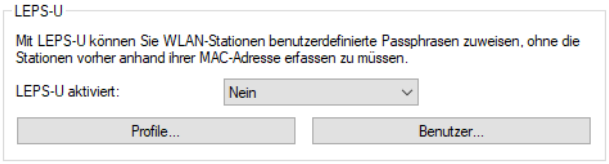
Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden" will, aber die Geräte nicht selber konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Preshared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Da LEPS-U ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Die Unsicherheit von globalen Passphrasen wird durch LEPS-U grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase „verloren geht" oder ein Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

Aus technischen Gründen ist LEPS-U nur mit der WPA-Version WPA2 kompatibel.

5.1 Stationen / LEPS

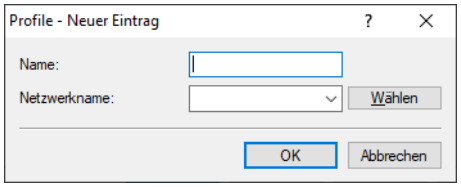
Die Konfiguration der **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security User (LEPS-U) finden Sie in LANconfig unter **Wireless-LAN** > **Stationen / LEPS** > **LEPS-U**. Über den Schalter **LEPS-U aktiviert** wird LEPS-U eingeschaltet.



Bei der Konfiguration von LEPS-U wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-U-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-U-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-U-Profile.

5.1.1 Profile

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden.



Name

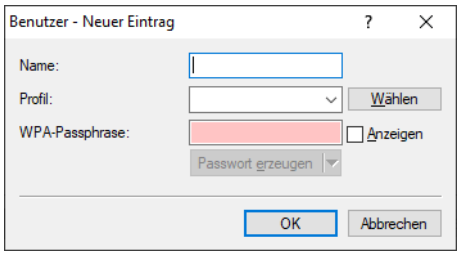
Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

Netzwerkname

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

5.1.2 Benutzer

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert.



Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

Profil

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

5.2 Ergänzungen im Setup-Menü

5.2.1 LEPS-U

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen.

SNMP-ID:

2.20.133

Pfad Konsole:

Setup > WLAN

Operating

Schaltet LEPS-U ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-U-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

SNMP-ID:

2.20.133.1

Pfad Konsole:

Setup > **WLAN** > **LEPS-U**

Mögliche Werte:

No
yes

Default-Wert:

No

Profiles

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

SNMP-ID:

2.20.133.2

Pfad Konsole:

Setup > **WLAN** > **LEPS-U**

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

SNMP-ID:

2.20.133.2.1

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Mögliche Werte:

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

Network-Name

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.20.133.2.2

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Mögliche Werte:

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

Users

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

SNMP-ID:

2.20.133.3

Pfad Konsole:

Setup > **WLAN** > **LEPS-U**

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

SNMP-ID:

2.20.133.3.1

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Users**

Mögliche Werte:

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

Profile

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.20.133.3.2

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Users**

Mögliche Werte:

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

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

SNMP-ID:

2.20.133.3.3

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Users**

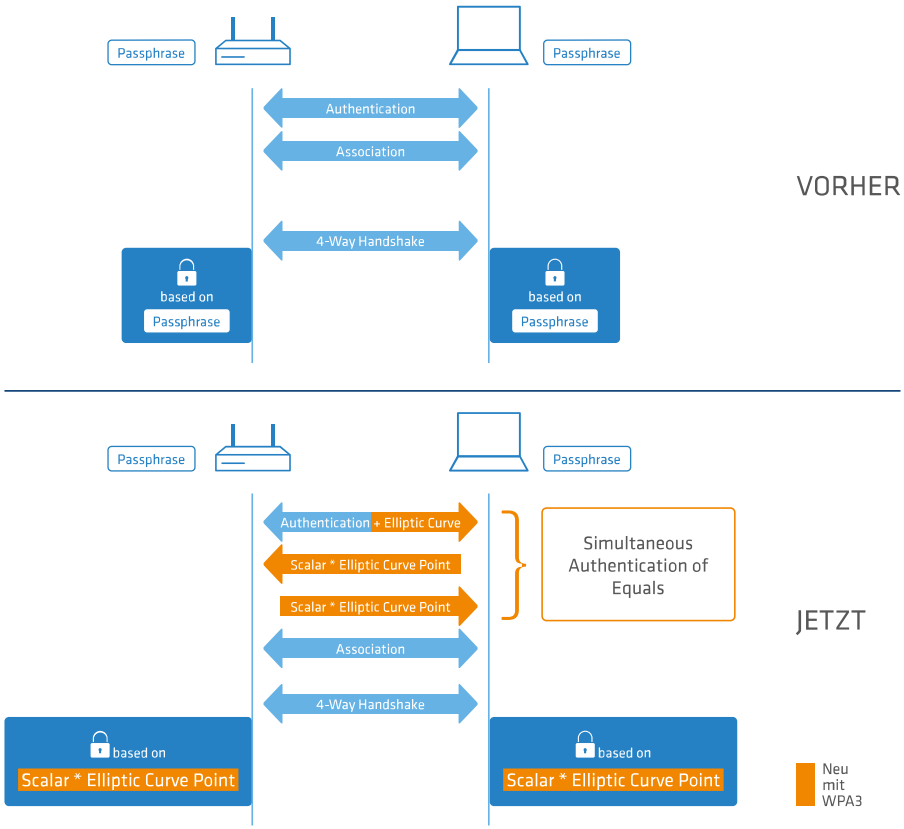
Mögliche Werte:

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

6 WPA3 (Wi-Fi Protected Access 3)

Der 2018 eingeführte WPA3-Standard der Wi-Fi-Alliance bietet gegenüber dem bereits 2004 eingeführten Vorgängerstandard WPA2 eine verbesserte Sicherheit durch eine Kombination verschiedener aktueller Sicherheitsverfahren. Wie WPA2 existiert auch WPA3 in den Ausprägungen WPA3-Personal und WPA3-Enterprise.

WPA3-Personal bietet durch die Verwendung des Authentisierungsverfahrens Simultaneous Authentication of Equals (SAE) eine Methode, die lediglich ein Passwort für die Authentifizierung voraussetzt und dennoch Brute-Force- und Wörterbuch-Attacken ins Leere laufen lässt. Zudem bietet dieses Verfahren erstmalig Forward Secrecy – dies bedeutet, dass in der Vergangenheit mitgeschnittener, WPA3-gesicherter Datenverkehr auch später nicht mehr entschlüsselt werden kann, wenn der Angreifer Kenntnis des Pre-Shared Keys erlangt.



Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA) Suite B-Kryptographie verwendet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

In beiden Varianten ist nun die Verwendung von Protected Management Frames (PMF) nach IEEE 802.11w verpflichtend. PMF verhindern, dass Angreifer durch Deassoziieren mittels gefälschter Management Frames und Belauschen der Wiederanmeldung Material bekommen, um das WLAN-Passwort zu errechnen.

6.1 WPA3-Personal

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Personal unterstützen; die Authentisierung wird mit dieser Konfiguration nur noch über Simultaneous Authentication of Equals (SAE) zugelassen. Ebenfalls wird für diese SSID nun die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

6.2 WPA3-Enterprise

WPA3-Enterprise ändert oder ersetzt die in WPA2-Enterprise definierten Protokolle nicht grundlegend. Stattdessen definiert es Richtlinien, um eine größere Konsistenz bei der Anwendung dieser Protokolle zu gewährleisten und die gewünschte Sicherheit zu gewährleisten.

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Enterprise unterstützen. Für diese SSID wird die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

Suite B-Kryptographie

Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA)-Suite-B-Kryptographie eingeschaltet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Es wird die Verwendung der folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und

ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Der im LCOS integrierte RADIUS-Server unterstützt die hier genannten Cipher-Suiten.

6.3 WPA3 konfigurieren

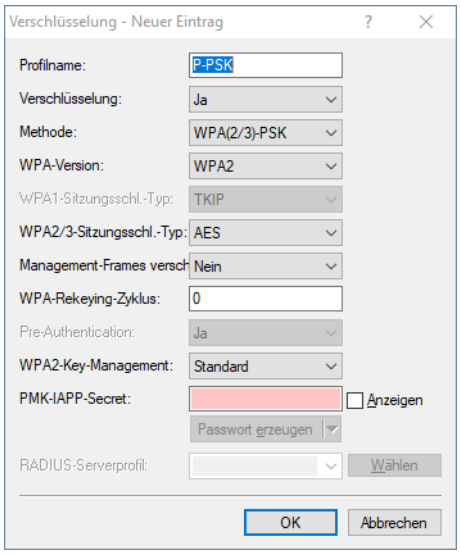
In LANconfig konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** alle notwendigen Einstellungen für WPA3. Zusätzlich sind folgende Verschlüsselungsprofile neu hinzugekommen und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

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.



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(2/3)-802.1X: WPA2 und / oder WPA3 mit 802.1X, auch bekannt als WPA-Enterprise

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP

Das Verfahren WEP bietet heutzutage keinerlei Vertraulichkeit mehr und sollte nur eingesetzt werden, um Legacy-Clients einzubinden, die kein neueres Sicherheitsverfahren unterstützen. In diesem Fall empfiehlt es sich, die WEP-Clients in einem eigenen VLAN vom Rest der WLAN-Infrastruktur zu isolieren.

- WEP-40-Bits: WEP mit Schlüssellänge 40 Bit
- WEP-104-Bits: WEP mit Schlüssellänge 104 Bit
- WEP-128-Bits: WEP mit Schlüssellänge 128 Bit
- WEP-40-Bits-802.1X: WEP mit Schlüssellänge 40 Bit und 802.1X

  Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.
- WEP-104-Bits-802.1X: WEP mit Schlüssellänge 104 Bit und 802.1X

  Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.
- WEP-128-Bits-802.1X: WEP mit Schlüssellänge 128 Bit und 802.1X

  Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

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.

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.

Management-Frames verschlüsseln

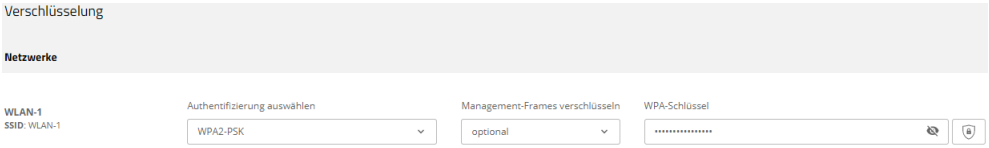
Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf „Mandatory (Obligatorisch)“ gesetzt angenommen. Bei WPA2 ist diese Option optional.

In WEBconfig ist dies über die Einstellungen im Bereich **Verschlüsselung** bei der jeweiligen SSID in der **WLAN-Konfiguration** möglich:

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



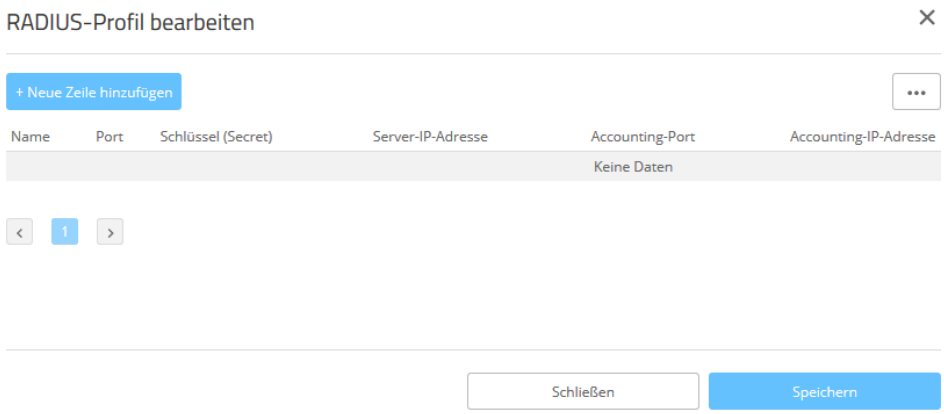
Authentifizierung auswählen

Ändern Sie hier die Verschlüsselungs- und Authentifizierungsmethode. Standardmäßig ist WPA2-PSK (WPA2 mit Pre-shared Key bzw. WPA2-Personal) voreingestellt. Wählen Sie optional **Keine Verschlüsselung** oder aus den folgenden Möglichkeiten:

- WPA3-PSK – WPA3 mit Pre-shared Key bzw. WPA3-Personal
- WPA(2+3)-PSK – WPA2 und / oder WPA3 mit Pre-Shared-Key
- WPA2-801.1X– WPA2 mit 802.1X bzw. WPA2-Enterprise
- WPA3-801.1X– WPA3 mit 802.1X bzw. WPA3-Enterprise
- WPA(2+3)-801.1X– WPA2 und / oder WPA3 mit 802.1X

Im Falle von Verfahren mit Pre-shared Key (PSK) müssen Sie einen **WPA-Schlüssel** eingeben. Schalten Sie die Anzeige über das durchgestrichene Auge um, damit Sie den Schlüssel lesen können. Je nach Bedarf ist es hier auch möglich, einen sicheren WPA-Schlüssel automatisch generieren zu lassen ( )

Im Falle von 802.1X müssen Sie ein RADIUS-Profil anlegen. Klicken Sie dazu auf **RADIUS-Profil bearbeiten** und fügen dort eine neue Zeile hinzu.



Name

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

Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Server zu kontaktieren.

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Schlüssel (Secret)

Konfigurieren Sie hier das Secret, mit welchem der Datenverkehr zwischen dem Gerät und dem RADIUS-Server verschlüsselt wird. Dieses Secret muss ebenfalls auf dem RADIUS-Server hinterlegt sein.

Server-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Server erreichbar ist.

Accounting-Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Accounting-Server zu kontaktieren.

Normalerweise ist dies der Port 1813 (RADIUS Accounting).

Accounting-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Accounting-Server erreichbar ist.

Beachten Sie, dass normalerweise dem RADIUS-Server das hier als RADIUS-Client agierende Gerät ebenfalls in seiner Konfiguration bekannt gemacht werden muss.

Sichern Sie die Änderungen durch Klick auf **Speichern**

Management-Frames verschlüsseln

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren

für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf **Notwendig** gesetzt angenommen. Bei WPA2 ist diese Option optional.

6.4 Ergänzungen im Setup-Menü

6.4.1 Method

Konfigurieren Sie hier die Verschlüsselungsmethode.

Das Verfahren WEP bietet heutzutage keinerlei Vertraulichkeit mehr und sollte nur eingesetzt werden, um Legacy-Clients einzubinden, die kein neueres Sicherheitsverfahren unterstützen. In diesem Fall empfiehlt es sich, die WEP-Clients in einem eigenen VLAN vom Rest der WLAN-Infrastruktur zu isolieren.

SNMP-ID:

2.20.3.4

Pfad Konsole:

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

Mögliche Werte:

WEP-40-Bits

WEP mit Schlüssellänge 40 Bit

WEP-104-Bits

WEP mit Schlüssellänge 104 Bit

WEP-128-Bits

WEP mit Schlüssellänge 128 Bit

WEP-40-Bits-802.1X

WEP mit Schlüssellänge 40 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-104-Bits-802.1X

WEP mit Schlüssellänge 104 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-128-Bits-802.1X

WEP mit Schlüssellänge 128 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

802.11i-WPA-PSK

WPA(2) mit Pre-Shared-Key

802.11i-WPA-802.1X

WPA(2) mit 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

Enhanced-Open

Hotspots werden bisher hauptsächlich unverschlüsselt betrieben, wodurch auf der Funkschnittstelle keinerlei Vertraulichkeit der übertragenen Daten gegeben ist. Auch die verbreitete Praxis, einen Hotspot mit WPA2-PSK abzusichern und den gemeinsamen Schlüssel etwa durch einen Aushang bekannt zu machen, bietet nur eingeschränkte Sicherheit. Da WPA2-PSK keine Perfect Forward Secrecy bietet, kann ein Angreifer, dem dieser Schlüssel bekannt ist, nachträglich damit abgesicherten Datenverkehr entschlüsseln. Das Enhanced Open-Verfahren kann verwendet werden, um diese Risiken zu minimieren. Es bietet verschlüsselte Kommunikation für alle Clients, die dieses Verfahren unterstützen, so dass nicht jeder in der gleichen Funkzelle alles einfach mitlesen kann. Es bleibt das Risiko einer Man-in-the-Middle-Attacke, aber im Vergleich zu einem unverschlüsselten offenen Hotspot ist es ein deutlich geringeres Risiko. Es muss nur die Verschlüsselungsmethode eingestellt werden. Mehr ist nicht notwendig, um die Kommunikation mit Clients, welche dieses Verfahren unterstützen, zu verschlüsseln.

6.4.2 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:

2.20.3.9

Pfad Konsole:

Setup > **WLAN** > **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.

6.4.3 WPA2-3-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 2 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:

2.20.3.13

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.

6.4.4 Prot.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf „Mandatory (Obligatorisch)“ gesetzt angenommen. Bei WPA2 ist diese Option optional.

SNMP-ID:

2.20.3.14

Pfad Konsole:

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

Mögliche Werte:

No

PMF nicht verwenden.

optional

PMF anbieten. Der Client entscheidet, ob diese verwendet werden.

mandatory

PMF verwenden.

6.4.5 SAE/OWE-Groups

Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen als Bitmaske, auf deren Basis die Protokollpartner einen Schlüssel für den Datenaustausch erstellen. Die vorhandenen Gruppen nutzen elliptische Kurven

Das bei WPA3 verwendete Authentisierungsverfahrens SAE (Simultaneous Authentication of Equals) nutzt diese Verfahren zusammen mit AES zur Erzeugung eines kryptographisch starken Schlüssels.

SNMP-ID:

2.20.3.26

Pfad Konsole:

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

Mögliche Werte:

DH-19

Bit 0x80000 (524288) – 256-bit random ECP group

DH-20

Bit 0x100000 (1048576) – 384-bit random ECP group

DH-21

Bit 0x200000 (2097152) – 521-bit random ECP group

Default-Wert:

DH-19

7 Auto Updater – Immer up-to-date

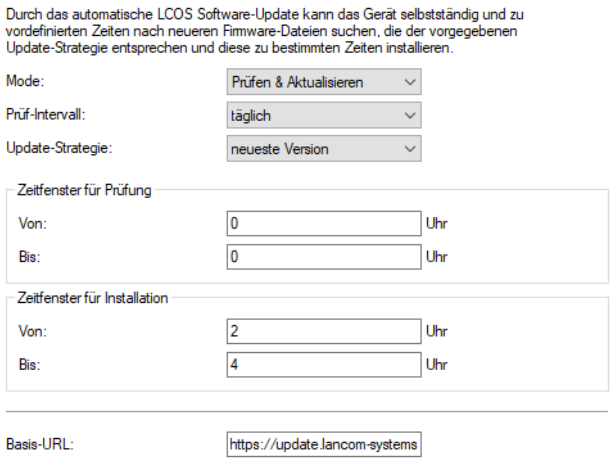
Der Auto Updater hält Ihre Installationen automatisch immer auf dem aktuellen Stand: LCOS LX-basierte Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Dabei wählen Sie, ob Sie nur Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden, die Sie anschließend mit einem Klick manuell installieren können.

7.1 Software-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff. 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.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

Die Konfiguration des LANCOM Auto Updaters finden Sie in LANconfig unter **Management** > **Software-Update**.



Mode

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater.
- Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server

aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS LX-Menübaum und via Syslog signalisiert.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manuell

- Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste Version ohne REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 REL.

Zeitfenster für Prüfung

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

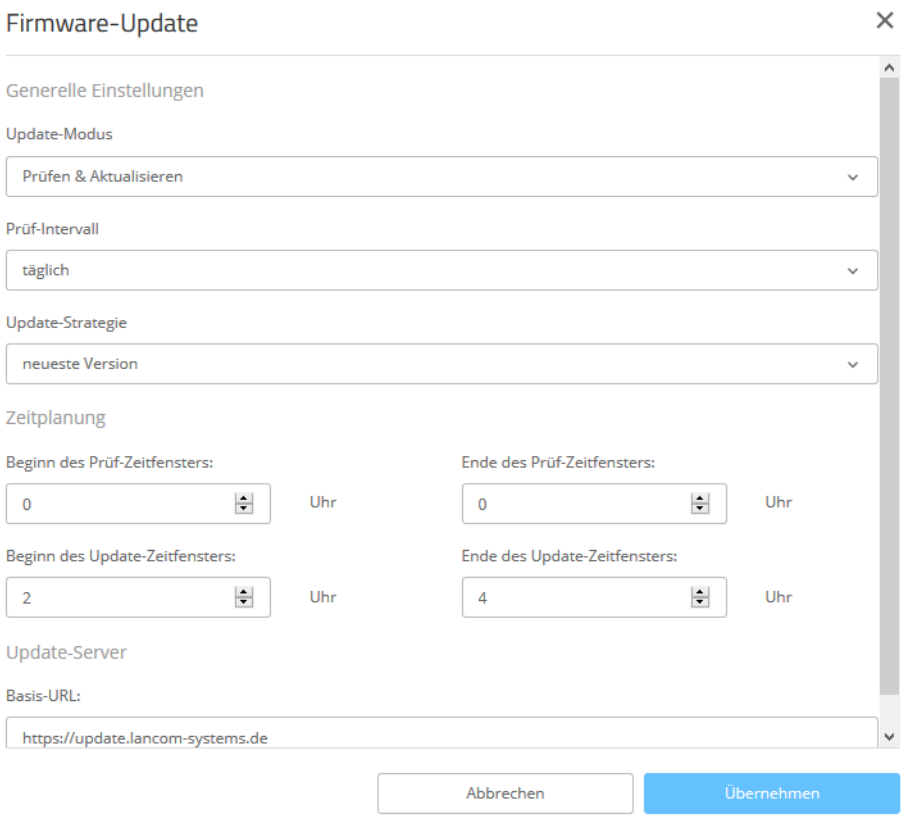
Zeitfenster für Installation

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

7.2 Automatisches Firmware Update



Update-Modus

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater.
- Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server

aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS LX-Menübaum und via Syslog signalisiert.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manuell

- Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber auch auf 5.00 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber nicht auf 5.00 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 SU1 aktualisiert, aber nicht auf 4.00 RU2.

neueste Version ohne REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 4.00 ist installiert; es wird auf 5.00 RU1 aktualisiert, aber nicht auf 5.00 REL.

Prüf-Zeitfenster

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden.

Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Update-Zeitfenster

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

7.3 Ergänzungen im Setup-Menü

7.3.1 Automatic-Firmware-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff (unattended). 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.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

SNMP-ID:

2.107

Pfad Konsole:

Setup

Mode

Stellen Sie hier den Betriebsmodus des LANCOM Auto Updaters ein.

SNMP-ID:

2.107.1

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

manual

Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.

Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS LX-Menübaum und via Syslog signalisiert. Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check-and-update

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Der Update-Server ermittelt anhand der Versions-Policy das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater. Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

Default-Wert:

check-and-update

Check-Firmware-Now

Dieser Befehl veranlasst das Gerät, zu prüfen, ob auf dem LANCOM Update-Server eine neuere Firmware vorhanden ist.

SNMP-ID:

2.107.2

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Update-Firmware-Now

Dieser Befehl veranlasst das Gerät, die neueste Firmware vom LANCOM Update-Server herunterzuladen und zu installieren.

SNMP-ID:

2.107.3

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Cancel-Current-Action

Dieser Befehl veranlasst das Gerät, die aktuelle laufende Aktion des Auto Updaters abzubrechen. Dies bezieht sich sowohl auf manuell gestartete als auch auf geplant ausgeführte Aktionen.

SNMP-ID:

2.107.4

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Reset-Updater-Config

Dieser Befehl setzt die auf den Auto Updater bezogenen bootpersistenten Konfigurationsdateien zurück. Dies schließt die lokale Blacklist ein, die Firmware-Versionen enthält, mit denen ein automatisches Update fehlgeschlagen ist.

SNMP-ID:

2.107.5

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Base-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

SNMP-ID:

2.107.6

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

max. 252 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default-Wert:

https://update.lancom-systems.de

Check-Interval

Der Auto Updater bestimmmt beim ersten Start einen zufälligen Zeitraum innerhalb eines Tages oder einer Woche, an dem die Prüfung durchgeführt wird. Das eigentliche Update soll dann im nächsten Zeitraum zwischen 2-4 Uhr (Voreinstellung) durchgeführt werden.

SNMP-ID:

2.107.7

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

daily
weekly

Default-Wert:

daily

Version-Policy

Stellen Sie hier die Versionsrichtlinie des LANCOM Auto Updaters ein. Diese steuert, welche Firmware-Versionen einem Gerät zum Update angeboten werden.

SNMP-ID:

2.107.8

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

latest
Releaseübergreifend immer die neueste Version. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber auch auf 5.00 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

current
Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber nicht auf 5.00 Rel.

security-updates-only
Innerhalb eines Releases das neueste SU. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 SU1 aktualisiert, aber nicht auf 4.00 RU2.

latest-without-REL
Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 4.00 ist installiert; es wird auf 5.00 RU1 aktualisiert, aber nicht auf 5.00 REL.

Default-Wert:

security-updates-only

Check-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

SNMP-ID:

2.107.10

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

Check-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

SNMP-ID:

2.107.11

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

Install-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

SNMP-ID:

2.107.12

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

2

Install-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

SNMP-ID:

2.107.13

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

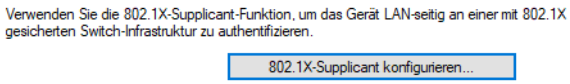
4

8 802.1X-Supplicant am LAN

Ab LCOS LX 5.10 können Sie den Access Point so konfigurieren, dass er sich an einer per 802.1X gesicherten Switch-Infrastruktur anmeldet.

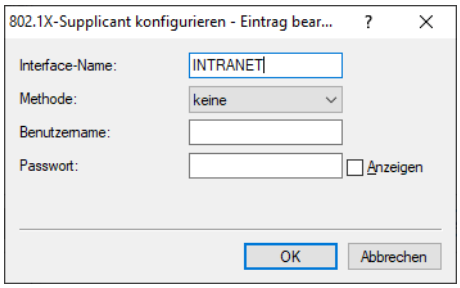
8.1 802.1X-Supplicant

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät LAN-seitig an einer mit 802.1X gesicherten Switch-Infrastruktur zu authentifizieren. Diese sind unter **Management** > **802.1X-Supplicant**.



8.1.1 802.1X-Supplicant konfigurieren

Die 802.1X-Supplicant-Funktionalität konfigurieren Sie unter **Management** > **802.1X-Supplicant** > **802.1X-Supplicant konfigurieren**.



Interface-Name

Der Name der LAN-Schnittstelle. Aktuell gibt es nur die Schnittstelle INTRANET, daher kann diese nicht geändert werden.

Methode

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

Benutzername

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

Passwort

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Die Unterstützung für eine Anmeldung mittels Client-Zertifikaten folgt in einer zukünftigen LCOS LX-Version.

8.2 Ergänzungen im Setup-Menü

8.2.1 Supplicant-Ifc-Setup

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät LAN-seitig an einer mit 802.1X gesicherten Switch-Infrastruktur zu authentifizieren.

SNMP-ID:

2.30.11

Pfad Konsole:

Setup > **IEEE802.1X**

Interface-Name

Der Name der LAN-Schnittstelle. Aktuell gibt es nur die Schnittstelle INTRANET, daher kann diese nicht geändert werden.

SNMP-ID:

2.30.11.1

Pfad Konsole:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

Method

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

SNMP-ID:

2.30.11.2

Pfad Konsole:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Mögliche Werte:

none
MD5
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

Username

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

SNMP-ID:

2.30.11.3

Pfad Konsole:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Mögliche Werte:

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

Password

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

SNMP-ID:

2.30.11.4

Pfad Konsole:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Mögliche Werte:

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

9 SNMPv3 mit LANmonitor-Support

Dieses Feature ermöglicht professionelle Netzwerküberwachung durch die Unterstützung von SNMPv3 (Simple Network Management Protocol Version 3). Damit ist auch das komfortable Geräte-Monitoring mit hoher Sicherheit, dank verschlüsselter Datenkommunikation, über den LANmonitor möglich.

Soll nach einem Update eines LANCOM LW-500 von LCOS LX 4.00 auf LCOS LX 5.10 das neue Feature SNMPv3 in Zusammenspiel mit dem root-Benutzer verwendet werden (z. B. durch LANmonitor), ist es erforderlich, das Hauptgerätepasswort erneut auf dem Gerät zu setzen. Das kann entweder über die WEBconfig, LANconfig oder die CLI erfolgen. Der Hintergrund ist, dass das Hauptgerätepasswort für die Verwendung mit SNMPv3 in einer mit SNMPv3-kompatiblen Form als Hashwert im Gerät hinterlegt werden muss. Dieser Vorgang erfolgt durch das erneute Setzen des Passworts.

Dieser Vorgang ist nur einmalig beim Upgrade von LCOS LX 4.00 auf eine höhere Version notwendig. Für zukünftige Upgrade-Schritte ist dies nicht erforderlich. Insbesondere zum Ermöglichen der Benutzung des LANmonitor sind die beschriebenen Schritte erforderlich!

9.1 Simple Network Management Protocol (SNMP)

9.1.1 SNMPv3-Grundlagen

Die Protokoll-Struktur von SNMP hat sich in der Version 3 grundlegend geändert. SNMPv3 ist in mehrere Module mit klar definierten Interfaces aufgeteilt, die untereinander kommunizieren. Die drei wichtigsten Elemente in SNMPv3 sind „Message Processing and Dispatch (MPD)“, „User-based Security Model (USM)“ und „View-based Access Control Mechanism (VACM)“.

MPD

Das MPD-Modul ist verantwortlich für die Verarbeitung (processing) und die Weiterbeförderung (dispatch) der ein- und ausgehenden SNMP-Meldungen.

USM

Das USM-Modul verwaltet Sicherheitsfunktionen, die die Authentifizierung der Nutzer sowie die Verschlüsselung und Integrität der Daten sicherstellen. SNMPv3 hat das Prinzip des „Security Models“ eingeführt, so dass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3“ zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model“ auszuwählen.

VACM

Der VACM stellt sicher, dass der Sender einer SNMP-Anfrage berechtigt ist, die angefragte Information zu erhalten. Die entsprechenden Zugriffsberechtigungen finden sich in den folgenden Einstellungen und Parametern:

SNMPv3-Views

„SNMPv3-Views“ fassen Inhalte, Statusmeldungen und Aktionen der Management Information Base (MIB) zusammen, die eine SNMP-Anfrage mit entsprechenden Zugriffsrechten erhalten bzw. ausführen darf. Diese Ansichten können einzelne Werte, aber auch komplette Pfade der MIB sein. Die Angabe dieser Inhalte erfolgt anhand der jeweiligen OIDs der MIB-Einträge.

Auf diese Weise erhält der Sender einer SNMP-Anfrage auch nach erfolgreicher Authentifizierung nur Zugriff auf die Daten, für die er gemäß SNMPv3-Views die Zugriffsrechte besitzt.

SNMPv3-Groups

„SNMPv3-Groups" fassen Nutzer mit gleichen Zugriffsrechten in einer jeweiligen Gruppe zusammen.

Security-Levels

„Security Levels" bestimmen die Sicherheitsstufe für den Austausch von SNMP-Nachrichten. Die folgenden Stufen sind auswählbar:

NoAuth-NoPriv

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

Auth-NoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

Auth-Priv

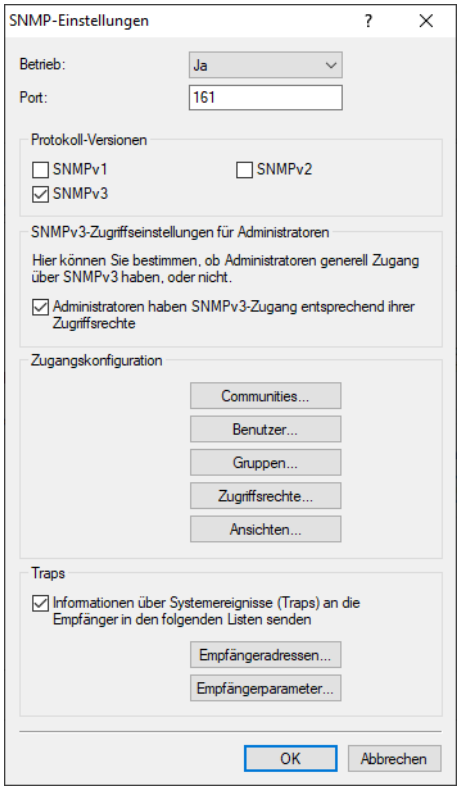
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Kontext

Der „Kontext" ist dafür vorgesehen, die einzelnen SNMP-Entities voneinander zu unterscheiden.

9.1.2 SNMP konfigurieren

Die SNMP-Einstellungen des Gerätes finden Sie unter **Management** > **Admin** > **SNMP** > **SNMP-Einstellungen**.



Betrieb

Aktivieren Sie SNMP für die im Folgenden angegebenen SNMP-Protokollversionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

Port

Passen Sie ggfs. den Port für SNMP an. Default: 161

Protokoll-Versionen

SNMPv1

Aktiviert SNMPv1.

SNMPv2

Aktiviert SNMPv2c.

SNMPv3

Aktiviert SNMPv3.

SNMPv3-Zugriffseinstellungen für Administratoren

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Zugangskonfiguration

SNMP-Communities

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten „Community", welche die Bedeutung eines Passworts bzw. Zugangsschlüssels inne hat. Die Authentifizierung kann hierbei wahlweise

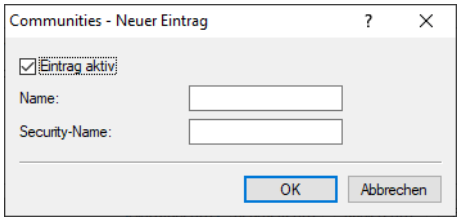
- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff),
- oder eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen.

Eine Communitiy fasst somit bestimmte SNMP-Hosts zu Gruppen zusammen, um diese einerseits einfacher verwalten zu können. Andererseits bieten SNMP-Communities eine eingeschränkte Sicherheit beim Zugriff über SNMP, da ein SNMP-Agent nur SNMP-Anfragen von Teilnehmern akzeptiert, deren Community ihm bekannt ist.

Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig eigene Communities zu definieren.

Diese Konfiguration ist nur für die SNMP-Versionen v1 und v2c relevant.



Eintrag aktiv

Aktiviert oder deaktiviert diese SNMP-Community.

Name

Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

Security-Name

Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.

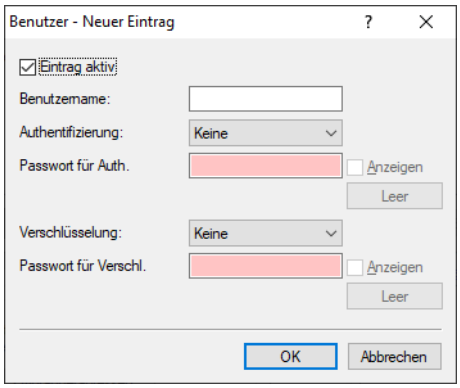
Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community. Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Benutzer

Neben den am Gerät registrierten Administratoren ist der Zugriff auch für einzelne Nutzer möglich. Hier konfigurieren Sie die Einstellungen für Authentifizierung und Verschlüsselung für diese Anwender bei Nutzung von SNMPv3.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Benutzer.

Benutzername

Vergeben Sie hier einen aussagekräftigen Namen für diesen Benutzer.

Authentifizierung

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss. Zur Verfügung stehen die folgenden Verfahren:

Keine

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA (Hash-Länge 160 Bits).

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

Passwort für Authentifizierung

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Verschlüsselung

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll. Zur Verfügung stehen die folgenden Verfahren:

Keine

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits)

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits)

AES256

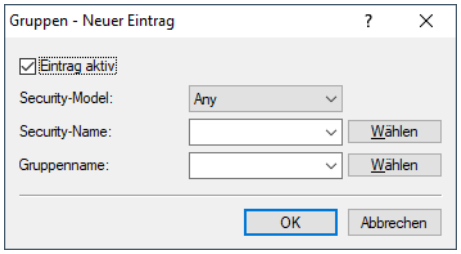
Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Passwort für Verschlüsselung

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Gruppen

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen. Als Standardeintrag ist die Konfiguration für den SNMP-Zugriff über den LANmonitor bereits voreingestellt.



Eintrag aktiv

Aktiviert oder deaktiviert diese Gruppe.

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

Any

Jedes Modell wird akzeptiert.

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „Keine Authentifizierung und keine Verschlüsselung".

SNMPv2_C

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „Keine Authentifizierung und keine Verschlüsselung".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind Sicherheitsstufen möglich, die bei den **Zugriffsrechten** aktiviert werden.

Security-Name

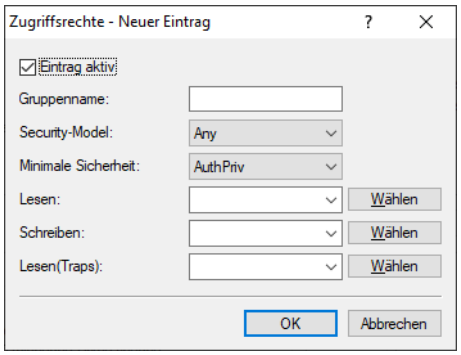
Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Gruppenname

Wählen Sie hier eine Gruppe aus, die Sie unter **Zugriffsrechte** definiert haben.

Zugriffsrechte

Diese Tabelle führt die verschiedenen Konfigurationen für Zugriffsrechte, Security-Modelle und Ansichten zusammen.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Gruppenname

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe.

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Minimale Sicherheit

Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Lesen

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access", „LANmonitor-Access", „Setup-Access" und „Status-Access".

Schreiben

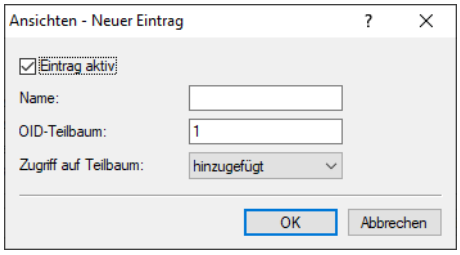
Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access", „LANmonitor-Access", „Setup-Access" und „Status-Access".

Lesen (Traps)

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte für Traps erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access", „LANmonitor-Access", „Setup-Access" und „Status-Access".

Ansichten

Hier fassen Sie verschiedene Werte oder ganze Zweige der MIB des Gerätes zusammen, die ein Benutzer gemäß seiner Zugriffsrechte einsehen oder verändern kann.



Eintrag aktiv

Aktiviert oder deaktiviert diese Ansicht.

Name

Vergeben Sie hier einen aussagekräftigen Namen für die Ansicht.

OID-Teilbaum

Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht ein- bzw. ausschließen soll.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

Zugriff auf Teilbaum

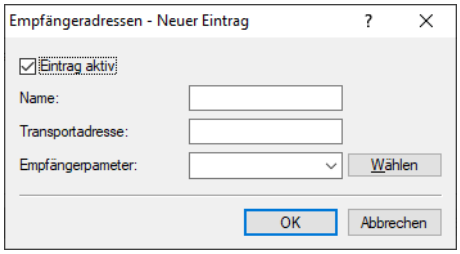
Bestimmen Sie, ob die angegebenen OID-Teilbäume Bestandteil („hinzugefügt") oder kein Bestandteil („entfernt") der Ansicht sind.

Traps

Wenn Sie die Option **Informationen über Systemereignisse (Traps) an die Empfänger in den folgenden Listen senden** aktivieren, dann bekommen die unter **Empfängeradressen** und **Empfängerparameter** konfigurierten Empfänger entsprechende Informationen.

Empfängeradressen

In der Liste der Empfängeradressen konfigurieren Sie die Empfänger, an die der SNMP-Agent die SNMP-Traps versendet.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Transportadresse

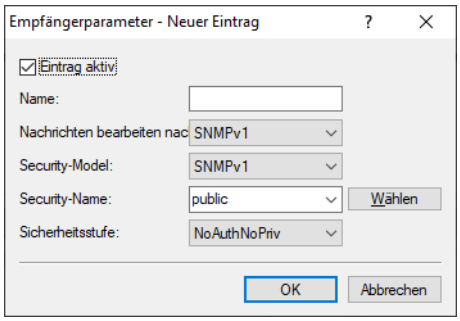
Konfigurieren Sie hier die Adresse des Empfängers. Diese Adresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax „<IP-Adresse>:<Port>" angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Empfängerparameter

Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.

Empfängerparameter

In dieser Tabelle konfigurieren Sie, wie der SNMP-Agent die SNMP-Traps behandelt, die er an die Empfänger versendet.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Nachrichten bearbeiten nach

Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, sodass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

Any

Jedes Modell wird akzeptiert.

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv2_C

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Dies kann ausschließlich zusammen mit SNMP-Benutzern gewählt werden. Die effektive mögliche Sicherheitsstufe hängt von den gewählten Authentifizierungs- und Verschlüsselungsmethoden des Benutzers ab.

Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Sicherheitsstufe

Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Trap beim Empfänger gelten soll.

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

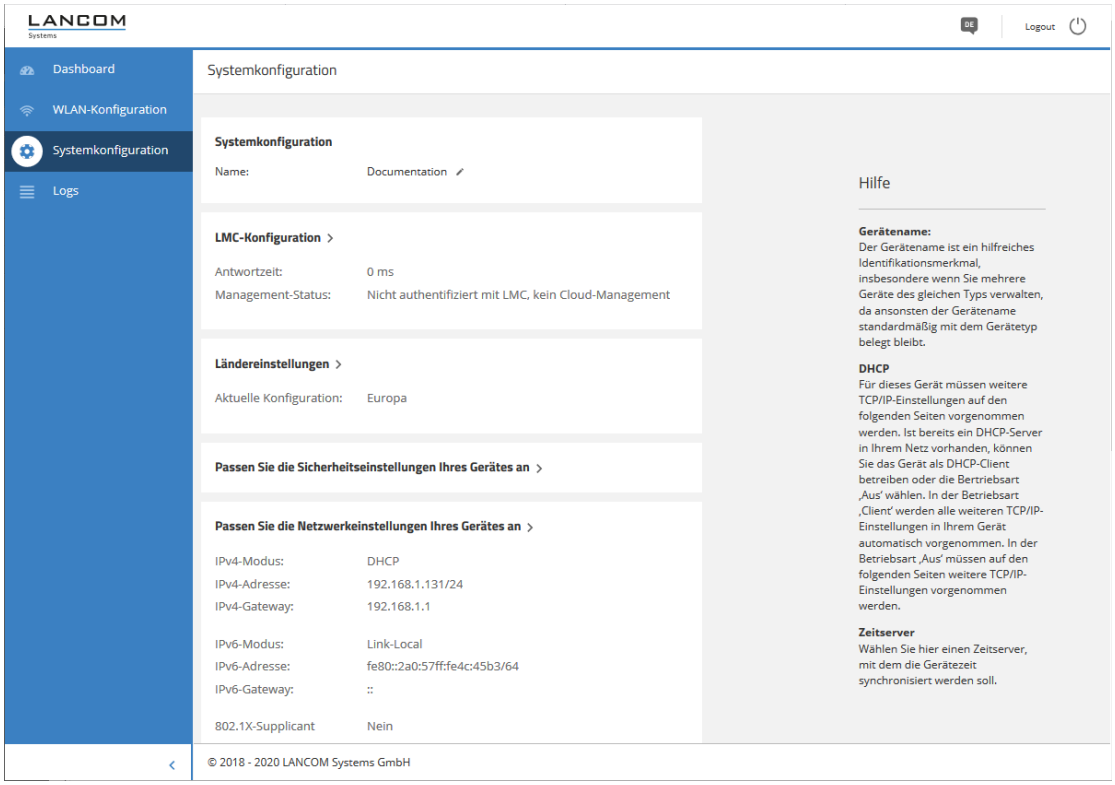
Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

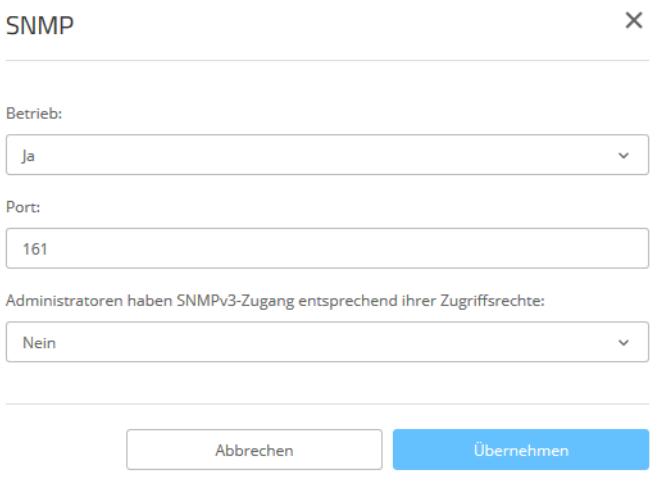
9.2 Systemkonfiguration

Die Systemkonfiguration bietet die Möglichkeit zur Konfiguration grundsätzlicher Parameter Ihres Gerätes, z. B. den Gerätenamen, die IP-Einstellungen zum Management des Gerätes oder die Aktivierung von SNMP.



Einzelne Felder wie den Systemnamen können Sie nach einem Klick auf den Haken neben diesem direkt bearbeiten. Für Bereiche öffnet sich eine Bearbeitungsmaske nach einem Klick auf die Überschrift.

9.2.1 SNMP



Betrieb

Aktivieren Sie SNMP.

Port

Passen Sie ggfs. den Port für SNMP an. Default: 161

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

9.3 Ergänzungen im Setup-Menü

9.3.1 SNMP

Dieses Menü enthält die Konfiguration von SNMP.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

SNMP-ID:

2.9

Pfad Konsole:

Setup

Send-Traps

Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der Tabelle Target-Addresses die Ziele ein, auf denen diese SNMP-Manager installiert sind.

SNMP-ID:

2.9.1

Pfad Konsole:

Setup > SNMP

Mögliche Werte:

Yes
No

Default-Wert:

No

Port

Über diesen Parameter legen Sie den Port fest, über den der SNMP-Dienst für externe Programme wie z. B. LANmonitor erreichbar ist.

SNMP-ID:

2.9.21

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

0 … 65535

Default-Wert:

161

Communities

SNMP-Agents und SNMP-Manager gehören SNMP-Communities an. Diese Communities fassen bestimmte SNMP-Hosts zu Gruppen zusammen, um diese einerseits einfacher verwalten zu können. Andererseits bieten SNMP-Communities eine eingeschränkte Sicherheit beim Zugriff über SNMP, da ein SNMP-Agent nur SNMP-Anfragen von Teilnehmern akzeptiert, deren Community ihm bekannt ist.

In dieser Tabelle konfigurieren Sie die SNMP-Communities.

Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

SNMP-ID:

2.9.27

Pfad Konsole:

Setup > **SNMP**

Name

Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

SNMP-ID:

2.9.27.1

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Security-Name

Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.

SNMP-ID:

2.9.27.3

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Status

Mit diesem Eintrag aktivieren oder deaktivieren Sie diese SNMP-Community.

SNMP-ID:

2.9.27.8

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

Active

Die Community ist aktiviert.

Inactive

Die Community ist deaktiviert.

Default-Wert:

Active

Groups

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen.

SNMP-ID:

2.9.28

Pfad Konsole:

Setup > SNMP

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen.

Entsprechend wählen Sie hier ein Security-Modell aus.

SNMP-ID:

2.9.28.1

Pfad Konsole:

Setup > SNMP > Groups

Mögliche Werte:

Any

Jedes Modell wird akzeptiert.

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv2_C

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind die folgenden Sicherheitsstufen möglich:

NoAuthNoPriv

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthNoPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Default-Wert:

SNMPv3_USM

Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

SNMP-ID:

2.9.28.2

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

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

Default-Wert:

leer

Group-Name

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe. Diesen Namen verwenden Sie anschließend bei der Konfiguration der Zugriffsrechte.

SNMP-ID:

2.9.28.3

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

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

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diese Gruppenkonfiguration.

SNMP-ID:

2.9.28.5

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Accesses

Diese Tabelle führt die verschiedenen Konfigurationen für Zugriffsrechte, Security-Models und Ansichten zusammen.

SNMP-ID:

2.9.29

Pfad Konsole:

Setup > **SNMP**

Group-Name

Wählen Sie hier den Namen einer Gruppe aus, für die diese Zugriffsrechte gelten sollen.

SNMP-ID:

2.9.29.1

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

SNMP-ID:

2.9.29.3

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Any

Jedes Modell wird akzeptiert.

SNMPv1

SNMPv1 wird verwendet.

SNMPv2_C

SNMPv2c wird verwendet.

SNMPv3_USM

SNMPv3 wird verwendet.

Default-Wert:

Any

Read-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.

SNMP-ID:

2.9.29.5

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

Write-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll.

SNMP-ID:

2.9.29.6

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

Notify-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Notify-Rechte erhalten soll.

SNMP-ID:

2.9.29.7

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diesen Eintrag.

SNMP-ID:

2.9.29.8

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Min-Security-Level

Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

SNMP-ID:

2.9.29.10

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

AuthPriv

Views

In dieser Tabelle fassen Sie verschiedene Werte oder ganze Zweige der MIB des Gerätes zusammen, die ein Benutzer gemäß seiner Zugriffsrechte einsehen oder verändern kann.

SNMP-ID:

2.9.30

Pfad Konsole:

Setup > **SNMP**

View-Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

SNMP-ID:

2.9.30.1

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

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

Default-Wert:

leer

OID-Subtree

Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht einschließen soll.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

SNMP-ID:

2.9.30.3

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

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

Default-Wert:

leer

Type

Bestimmen Sie, ob die nachfolgend angegebenen OID-Teilbäume Bestandteil („Included“) oder kein Bestandteil („Excluded“) der Ansicht sind.

SNMP-ID:

2.9.30.4

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Included

Diese Einstellung gibt MIB-Werten mit aus.

Excluded

Diese Einstellung blockt die Ausgabe von MIB-Werten.

Default-Wert:

Included

Status

Aktiviert oder deaktiviert diese Ansicht.

SNMP-ID:

2.9.30.6

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Users

Dieses Menü enthält die Benutzerkonfiguration.

SNMP-ID:

2.9.32

Pfad Konsole:

Setup > **SNMP**

Username

Geben Sie hier den SNMPv3 Benutzernamen an.

SNMP-ID:

2.9.32.2

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

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

Default-Wert:

leer

Authentication-Protocol

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss.

SNMP-ID:

2.9.32.5

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-96 (Hash-Länge 160 Bits).

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

Authentication-Password

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.14 Authentication-Password-Type* auf Seite 81 geändert wird.

SNMP-ID:

2.9.32.6

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `anything printable`

Default-Wert:

leer

Privacy-Protocol

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll.

SNMP-ID:

2.9.32.8

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits).

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits).

AES256

Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Privacy-Password

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.15 Privacy-Password-Type* auf Seite 81 geändert wird.

SNMP-ID:

2.9.32.9

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diesen Benutzer.

SNMP-ID:

2.9.32.13

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Authentication-Password-Type

Das Passwort in *2.9.32.6 Authentication-Password* auf Seite 79 wird immer verschlüsselt abgelegt (Typ „Masterkey"). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext" ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey" zurücksetzen.

SNMP-ID:

2.9.32.14

Pfad Konsole:

Setup > SNMP > Users

Mögliche Werte:

Plaintext
Masterkey

Privacy-Password-Type

Das Passwort in *2.9.32.9 Privacy-Password* auf Seite 80 wird immer verschlüsselt abgelegt (Typ „Masterkey"). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext" ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey" zurücksetzen.

SNMP-ID:

2.9.32.15

Pfad Konsole:

Setup > SNMP > Users

Mögliche Werte:

Plaintext
Masterkey

Target-Addresses

In der Liste der Empfängeradressen konfigurieren Sie die Empfänger, an die der SNMP-Agent die SNMP-Traps versendet.

SNMP-ID:

2.9.34

Pfad Konsole:

Setup > **SNMP**

Name

Geben Sie hier den Ziel-Adress-Namen an.

SNMP-ID:

2.9.34.1

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

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

Default-Wert:

leer

Transport-Address

Die Transportadresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax <IP-Adresse>:<Port> angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

SNMP-ID:

2.9.34.3

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

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

Default-Wert:

leer

Parameters-Name

Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.

SNMP-ID:

2.9.34.7

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

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

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diese Zieladresse.

SNMP-ID:

2.9.34.9

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Target-Params

In dieser Tabelle konfigurieren Sie, wie der SNMP-Agent die SNMP-Traps behandelt, die er an die Empfänger versendet.

SNMP-ID:

2.9.35

Pfad Konsole:

Setup > **SNMP**

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

SNMP-ID:

2.9.35.1

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

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

Default-Wert:

leer

Message-Processing-Model

Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.

SNMP-ID:

2.9.35.2

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

SNMPv1
SNMPv2c
SNMPv3

Default-Wert:

SNMPv3

Security-Model

Legen Sie mit diesem Eintrag das Sicherheitsmodell fest.

SNMP-ID:

2.9.35.3

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default-Wert:

SNMPv3_USM

Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

SNMP-ID:

2.9.35.4

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

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

Default-Wert:

leer

Security-Level

Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Traps beim Empfänger gelten soll.

SNMP-ID:

2.9.35.5

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Meldung ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

NoAuthNoPriv

Status

Aktiviert oder deaktiviert diesen Eintrag.

SNMP-ID:

2.9.35.7

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

Admitted-Protocols

Aktivieren Sie hier die SNMP-Versionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

SNMP-ID:

2.9.37

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

SNMPv1
SNMPv2
SNMPv3

Default-Wert:

SNMPv3

Allow-Admins

Sollen registrierte Administratoren (darunter fällt auch der Benutzer root) auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

SNMP-ID:

2.9.38

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
Yes

Default-Wert:

No

Operating

Dieser Eintrag aktiviert oder deaktiviert SNMP-Traps.

SNMP-ID:

2.9.41

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
SNMP-Traps sind ausgeschaltet.

Yes
SNMP-Traps sind eingeschaltet.

Default-Wert:

No