connecting your business



# Addendum LCOS 9.18 RU1



# Inhalt

1	Addendum zur LCOS-Version 9.18 RU1	4
2	Konfiguration	5
	2.1 Speicherung von Passwort-Formularfeldern im Browser verhindern	5
	2.1.1 Speicherung von Passwort-Formularfeldern im Browser verhindern	5
	2.1.2 Ergänzungen im Setup-Menü	5
	2.2 Vendor-DHCP-Option für LSR-Rollout im DHCP-Client	6
	2.2.1 LSR-Informationen über DHCP-Server erhalten	6
	2.2.2 Ergänzungen im Setup-Menü	8
3	WLAN	14
	3.1 Adaptive RF Optimization	14
	3.1.1 Adaptive RF Optimization mit LANconfig konfigurieren	14
	3.1.2 Ergänzungen im Setup-Menü	16
	3.2 Airtime Fairness	19
	3.2.1 Airtime Fairness mit LANconfig konfigurieren	20
	3.2.2 Ergänzungen im Setup-Menü	21
	3.3 Verschlüsseltes OKC über IAPP	21
	3.3.1 Verschlüsseltes OKC über IAPP	22
	3.3.2 Ergänzungen im Setup-Menü	22
	3.4 Fast Roaming	23
	3.4.1 Fast Roaming über IAPP	23
	3.4.2 Ergänzungen im Setup-Menü	24
	3.5 Wireless Intrusion Detection System (WIDS)	24
	3.5.1 WIDS mit LANconfig konfigurieren	25
	3.5.2 Ergänzungen im Setup-Menü	27
	3.6 Status-Zähler für fehlgeschlagene WPA-PSK / IEEE802.1X-Anmeldevorgänge	47
	3.6.1 Status-Zähler für WPA-PSK Anmeldevorgänge	47
	3.6.2 Status-Zähler für IEEE 802.1X-Anmeldevorgänge	48
	3.6.3 Ergänzungen im Status-Menü	48
	3.7 Adaptive Transmission Power	50
	3.7.1 Adaptive Transmission Power mit LANconfig konfigurieren	50
	3.7.2 Ergänzungen im Setup-Menü	51
	3.8 Erweiterte Startbedingungen für WLAN-RADIUS-Accounting	52
	3.8.1 Startbedingungen für RADIUS-Accounting mit LANconfig konfigurieren	53
	3.8.2 Startbedingungen für RADIUS-Accounting mit WEBconfig konfigurieren	53
	3.9 Auswahl eines RADIUS-Server-Profils bei Authentifizierung nach 802.1X	54
	3.9.1 Ergänzungen im Setup-Menü	54
	3.10 Konfigurierbare Datenraten pro WLAN-Modul	54
	3.10.1 Konfigurierbare Datenraten je WLAN-Modul	55
	3.10.2 Ergänzungen im Setup-Menü	57
4	WLAN-Management	88

4.1 IAPP bei bestehendem CAPWAP-Tunnel automatisch abschalten	88
5 LANCOM Location Based Services (LBS)	89
5.1 Dynamische und persistente Tracking-Listen von WLAN Clients	89
5.1.1 LBS-Tracking-Listen von Public-Spot-Benutzern verwenden	90
5.1.2 Ergänzungen im Setup-Menü	91
6 RADIUS	93
6.1 Benutzerdefinierbare Attribute im RADIUS-Client	93
6.2 Zugriffsinformationen auf den RADIUS-Server automatisch bereinigen	94
6.2.1 Ergänzungen im Setup-Menü	94
6.3 Vendor Specific RADIUS-Attribut "LCS-Routing-Tag"	95
7 Public Spot	96
7.1 Kürzere Einheiten für absolute Ablaufzeit	96
7.1.1 Kürzere Einheiten mit LANconfig konfigurieren	96
7.2 Circuit-ID als Public Spot-URL-Redirect-Variable	96
7.2.1 URL-Redirect Variable verwenden	96
7.3 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen	96
7.3.1 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen	97
7.3.2 Ergänzungen im Setup-Menü	97
7.4 PMS-Template: AGBs akzeptieren	98
7.5 Felder im Setup-Wizard "Public-Spot-Benutzer verwalten" ausblenden	98
7.5.1 Felder mit WEBconfig ausblenden	98
7.6 Redirect für HTTPS-Verbindungen umschaltbar	106
7.6.1 Redirect für HTTPS-Verbindungen	106
7.6.2 Ergänzungen im Setup-Menü	107
7.7 Ausgabe des Bandbreitenprofils auf dem Voucher	108
7.8 Template-Vorschau	108
7.8.1 Template-Vorschau über WEBconfig	109
7.9 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren	109
7.9.1 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren	110
7.9.2 Ergänzungen im Setup-Menü	110
7.10 Schutz vor Brute Force-Angriffen	114
7.10.1 Schutz vor Brute Force-Angriffen	114
7.10.2 Ergänzungen im Setup-Menü	115
8 Routing und WAN-Verbindungen	118
8.1 Route-Monitor	118
8.1.1 Route-Monitor	118
8.1.2 Ergänzungen im Setup-Menü	119
8.2 DiffServ-Feld per Default aktiviert	123
8.2.1 Ergänzungen im Setup-Menü	123
9 Weitere Dienste	124
9.1 IPv6-Unterstützung durch (S)NTP-Client und -Server	124

1 Addendum zur LCOS-Version 9.18 RU1

# 1 Addendum zur LCOS-Version 9.18 RU1

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 9.18 RU1 gegenüber der vorherigen Version.

# 2 Konfiguration

# 2.1 Speicherung von Passwort-Formularfeldern im Browser verhindern

Ab LCOS-Version 9.18 RU1 besteht die Möglichkeit, im Webbrowser die Speicherung von Passworten im Login-Formularfeld von WEBconfig zu unterdrücken.

# 2.1.1 Speicherung von Passwort-Formularfeldern im Browser verhindern

Eingabe-Dialoge auf Webseiten bieten den Webbrowsern die Möglichkeit, eingegebene Passwörter zu speichern, um sie bei einem erneuten Seitenaufruf komfortabel abzurufen. Diese Funktion der Webbrowser erleichtert Schadsoftware das Auslesen der vertraulichen Formulardaten.

Um die manuelle Eingabe des Login-Passworts bei jedem erneuten Seitenaufruf zu erzwingen, deaktivieren Sie im WEBconfig unter **Setup** > **HTTP** > **Verhindere-Passwort-Vervollstaendigung** die Speicherung von Formularfeld-Inhalten mit der Einstellung "Ja".

# 2.1.2 Ergänzungen im Setup-Menü

# Verhindere-Passwort-Vervollstaendigung

Konfigurieren Sie, ob der WEBconfig-Login-Dialog dem Browser des Anwenders erlaubt, den Inhalt des Passwort-Formularfeldes zur späteren Autovervollständigung zu speichern.

### SNMP-ID:

2.21.22

### **Pfad Telnet:**

Setup > HTTP

### Mögliche Werte:

### nein

Der Browser darf den Inhalt des Passwort-Formularfeldes nicht speichern. Die Eingabe-Maske von WEBconfig erzwingt somit die manuelle Eingabe des Passwortes durch den Anwender.

ja

Der Browser speichert die Eingabe des Passwort-Formularfeldes und füllt das Feld bei einem erneuten Aufruf des Login-Dialogs automatisch.

### **Default-Wert:**

nein

# 2.2 Vendor-DHCP-Option für LSR-Rollout im DHCP-Client

Ab Version 9.18 RU1 überträgt LCOS im unkonfigurierten Zustand über die Vendor spezifische DHCP-Option 43 LSR-Informationen an den DHCP-Server, der daraufhin die Kontaktinformationen für das LSR an das Gerät sendet.



Folgende LANCOM-Geräte unterstützen diese Funktion: L-3xx, L-4xx, L-13xx, L-151 LN-830, L-822, 178x-Serie, OAPs, IAPs, WLCs, 7100(+), 9100(+), 831A, 1631E, E-Serie.

# 2.2.1 LSR-Informationen über DHCP-Server erhalten

Ein unkonfiguriertes LANCOM-Gerät startet mit einem aktivierten DHCP-Client und bezieht dadurch IP-Adresse, Netzmaske, DNS-Adresse und Gateway-Adresse vom DHCP-Server im Netzwerk.

Über die Vendor spezifische DHCP-Option 43 sendet ein entsprechend konfigurierter DHCP-Server u. a. auch Informationen darüber, wie ein LSR-Server (Large Scale Rollout) zu erreichen ist. Der Rollout-Agent des LANCOM-Geräts wertet diese Information aus, kontaktiert den LSR-Server und bezieht anschließend im Rahmen der bestehenden Rollout-Strategie seine Konfiguration oder aktualisiert sein Firmware etc.

Diese Funktion erleichtert den Rollout-Prozess, da keine Vorkonfiguration der Geräte mehr notwendig ist. Die LSR-Informationen lassen sich auch durch entsprechende Variablen zusammensetzen, so dass der Betrieb ohne zentrales Rollout-System (LSR) möglich ist.

Die Verbindung zum LSR-Server erfolgt über HTTP, HTTPS oder TFTP, wobei im LANCOM-Gerät für eine sichere Verbindung ein entsprechendes SSL-Zertifikat gespeichert sein muss.

Eine Vorkonfiguration des Rollout-Agents ist weiterhin möglich. Der Empfang der LSR-Informationen stellt in diesem Fall sicher, dass das LANCOM-Gerät z. B. die aktuelle Adresse des LSR-Servers erhält.

# Konfiguration mit LANconfig

Mit LANconfig konfigurieren Sie den Rollout-Agent über Management > Rollout-Agent.

Rollout-Agent		
Betriebsart:	DHCP-gesteuert -	]
Wählen Sie die Betriebsar Rollout-Server senden, die übertragen wurden. Wählen Sie die Betriebsar Rollout-Server zu senden.	t "DHCP-gesteuert", wird der Ro vom DHCPv4-Server in der DH t "aktiv", um die hier konfigurierte	llout-Agent Attribute an den CP-Option 43 an das Gerät en Attribute an den
Rollout-Server (Konfiguration):		]
Rollout-Server (Firmware):		]
HTTP-Benutzername:		]
HTTP-Passwort:		Anzeigen
	Passwort <u>e</u> rzeugen	]
Projektnummer:		]
Weitere URL-Parameter:		]
TAN:		Anzeigen
	Passwort <u>e</u> rzeugen	]
Gerätenummer:		]
Neustart-Zeit:	0	Minuten
Anfrage-Intervall:	0	Minuten
Anfrage-Verzögerung:	0	Minuten
🦳 Anfrage-Verzögerungen zufälli	g verteilen	

### Betriebsart

Wählen Sie die Betriebsart "DHCP-gesteuert", wenn der Rollout-Agent des Gerätes die Attribute an den Rollout-Server übertragen soll, die er zuvor über die Vendor spezifische DHCP-Option 43 vom DHCP-Server erhalten hat. In der Betriebsart "Aktiv" überträgt das Gerät die in diesem Dialog konfigurierten Attribute. Die Betriebsart "Aus" deaktiviert den Rollout-Agenten.

Die Betriebsart "DHCP-gesteuert" überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

### **Rollout-Server (Konfiguration)**

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

Ein Eintrag ist möglich in der folgenden Form:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

### **Rollout-Server (Firmware)**

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

(i) Ein Eintrag ist möglich in der folgenden Form:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

### **HTTP-Benutzername**

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

# **HTTP-Passwort**

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

### Projektnummer

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

### Weitere URL-Parameter

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

### TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

### Gerätenummer

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

### Neustart-Zeit

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

### Anfrage-Intervall

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.

(i)

Bei einem Wert "0" startet der erneute Versuch in 1 Minute.

### Anfrage-Verzögerung

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

### Anfrage-Verzögerung zufällig verteilen

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

# 2.2.2 Ergänzungen im Setup-Menü

# **Rollout-Agent**

In diesem Menü konfigurieren Sie die Einstellungen des Rollout-Agenten.

#### SNMP-ID:

2.11.92

Pfad Telnet: Setup > Config

### Aktiviert

Mit diesem Eintrag legen Sie die Funktionsweise des Rollout-Agenten fest.

### SNMP-ID:

2.11.92.1

### Pfad Telnet:

Setup > Config > Rollout-Agent

### Mögliche Werte:

#### Nein

Der Rollout-Agent ist deaktiviert.

### Ja

Der Rollout-Agent ist aktiviert und überträgt die im Gerät konfigurierten Rollout-Daten an den Rollout-Server.

### **DHCP-initiiert**

Der Rollout-Agent ist aktiviert. Er wertet die Informationen aus, die er über den DHCP-Server in der DHCP-Option 43 erhalten hat.

Die Betriebsart "DHCP-initiiert" überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

### **Default-Wert:**

DHCP-initiiert

# **Konfigurations-Server**

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

(i) Ein Eintrag ist möglich in der folgenden Form:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

### SNMP-ID:

2.11.92.2

### **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

## **Firmware-Server**

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

(i) Ein Eintrag ist möglich in der folgenden Form:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

### SNMP-ID:

2.11.92.3

# **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

### Addendum

### 2 Konfiguration

### Username

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

### SNMP-ID:

2.11.92.4

### Pfad Telnet:

Setup > Config > Rollout-Agent

# Mögliche Werte:

```
max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

### **Default-Wert:**

leer

### Passwort

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

### SNMP-ID:

2.11.92.5

### **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

# **Projekt-Nummer**

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

### SNMP-ID:

2.11.92.6

### **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

### **Zusaetzliche-Parameter**

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

### SNMP-ID:

2.11.92.7

### **Pfad Telnet:**

Setup > Config > Rollout-Agent

# Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

# **Reboot-Zeit**

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

### SNMP-ID:

2.11.92.8

### **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 10 Zeichen aus [0-9]

### **Default-Wert:**

0

### **Request-Interval**

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.

### SNMP-ID:

2.11.92.9

### Pfad Telnet:

Setup > Config > Rollout-Agent

### Mögliche Werte:

max. 10 Zeichen aus [0-9]

### **Default-Wert:**

0

### Addendum

2 Konfiguration

### **Besondere Werte:**

0

Der erneute Versuch startet in 1 Minute.

# TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

### SNMP-ID:

2.11.92.10

# **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

```
max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

### **Default-Wert:**

leer

# **Geraete-Nummer**

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

#### SNMP-ID:

2.11.92.11

# **Pfad Telnet:**

Setup > Config > Rollout-Agent

# Mögliche Werte:

max. 255 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()\*+-,/:;<=>?[\]^\_. `

### **Default-Wert:**

leer

### **Request-Verzoegerung**

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

# SNMP-ID:

2.11.92.12

# **Pfad Telnet:**

Setup > Config > Rollout-Agent

# 2 Konfiguration

### Mögliche Werte:

max. 10 Zeichen aus [0-9]

### **Default-Wert:**

0

# **Request-Zeit-Verteilung**

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

### SNMP-ID:

2.11.92.13

# **Pfad Telnet:**

Setup > Config > Rollout-Agent

# Mögliche Werte:

Nein Ja

### **Default-Wert:**

Nein

### Zertifikats-Check-unterlassen

Legt fest, ob bei HTTPS-Verbindungen eine Überprüfung des Server-Zertifikats erfolgen soll.

### SNMP-ID:

2.11.92.14

#### **Pfad Telnet:**

Setup > Config > Rollout-Agent

### Mögliche Werte:

#### Nein

Ein Zertifikats-Check wird durchführt.

Ja

Es wird kein Zertifikats-Check durchgeführt.

# **Default-Wert:**

Nein

# 3 WLAN

# 3.1 Adaptive RF Optimization



Höherer WLAN-Durchsatz dank dynamischer Auswahl des qualitativ besten WLAN-Kanals durch den Access Point bei Kanalstörungen.

Mit der Auswahl des WLAN-Kanals wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Um in der Funkreichweite eines anderen APs ein WLAN störungsfrei betreiben zu können, sollte jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen (Shared Medium). Zu diesem Zweck nutzen LANCOM APs das Feature Adaptive RF Optimization. Dabei scannt der AP permanent das Funkfeld auf Störsignale. Wird ein bestimmter Schwellwert (auf Basis der "Wireless Quality Indicators") im aktuell verwendeten WLAN-Kanal überschritten, wechselt der AP automatisch auf einen qualitativ besseren Kanal. Diese intelligente Funktion ermöglicht es dem AP, sich an ein sich veränderndes Funkfeld dynamisch anzupassen, um somit die Robustheit des WLANs zu maximieren.

Sie haben in LANconfig die Möglichkeit, die Schwellwerte, die zu einem automatischen Kanalwechsel führen, manuell festzulegen.

() Mit der aktuellen LCOS-Version ist die Verwendung der Adaptive RF Optimization auf folgenden Geräten möglich: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, LA-3xx, IAP-3xx, OAP-3xx, OAP-8xx.

# 3.1.1 Adaptive RF Optimization mit LANconfig konfigurieren



Um die Funktion Adaptive RF Optimization über LANconfig konfigurieren zu können, ist es erforderlich, dass die zu konfigurierenden Geräte das Feature "Wireless Quality Indicators" anbieten. Weitere Informationen zu WQI entnehmen Sie bitte dem Referenzhandbuch. Um die Adaptive RF Optimization mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt "Interfaces" auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Adaptive RF Optimization**.

Adaptive RF Optimization aktivit	eren	iwechsel volgenommen wild.
Schwellwerte		
Minimale Client-Signal-Stärke:	15	%
Mindest-Paketanzahl an Client:	30	
Paket-Wiederholrate zu Client:	70	%
Obere Rausch-Schranke:	-70	dBm
Dauer der Kanalblockierung:	20	Minuten
Minimaler Auslösezeitraum:	1	Minuten

#### Adaptive RF Optimization aktivieren

Um die Überwachung der WLAN-Umgebung durch die Adaptive RF Optimization zu aktivieren, markieren Sie die Option Adaptive RF Optimization aktivieren.

Konfigurieren Sie anschließend die Schwellwerte, die einen automatischen Kanalwechsel auslösen sollen.

### Minimale Client-Signal-Stärke

Definieren Sie die minimale Signalstärke, mit der ein Client gesehen werden muss. Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein. Die Angabe erfolgt in % (Defaultwert: 15).

### **Mindest-Paketanzahl an Client**

Geben Sie an, wie viele Pakete mindestens an einen Client gesendet werden müssen (TX). Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein (Defaultwert: 30).

### Paket-Wiederholrate zu Client

Hier definieren Sie die Obergrenze der Paket-Wiederholrate zu Clients. Hat ein Client mehr als die hier angegebene Prozentzahl an Paketen erhalten, berücksichtigt das Gerät diesen Client bei der Entscheidung für einen Kanalwechsel. Die Angabe erfolgt in % (Defaultwert: 70).

### **Obere Rausch-Schranke**

Definieren Sie die Obergrenze des zulässigen Kanalrauschens. Die Angabe erfolgt in dBm (Defaultwert: -70).

### Dauer der Kanalblockierung

Wird ein Kanal als unbrauchbar erkannt, wird er für diese Zeit markiert / blockiert. Dieser Wert steuert auch die Blockierungszeit des Kanalwechseltriggers, falls alle Kanäle gleichzeitig blockiert sind. Die Angabe erfolgt in Minuten (Defaultwert: 20).

### Minimaler Auslösezeitraum

Geben Sie an, für wie lange ein Limit überschritten sein muss, bevor das Gerät eine Aktion auslöst. Erfolgt pro Periode (20 Sekunden) keine Limitüberschreitung, setzt das Gerät die abgelaufene Zeit zurück. Bei einer Limitüberschreitung über den gesamten angegebenen Zeitraum markiert / blockiert das Gerät den Kanal. Die Angabe erfolgt in Minuten (Defaultwert: 1).

Für diesen Wert empfehlen sich kleine einstellige Werte.

# 3.1.2 Ergänzungen im Setup-Menü

(!)

# Adaptive-RF-Optimization

Die **Adaptive RF Optimization** beobachtet und bewertet auf Basis der "Wireless Quality Indicators"-Kenngrößen permanent die WLAN-Umgebung und kann so die Qualität des Netzwerkes bestimmen. Nimmt die Qualität des Netzwerkes ab, sucht die Adaptive RF Optimization nach einem neuen Kanal, der für den Betrieb besser geeignet ist.

### SNMP-ID:

2.23.20.23

Pfad Telnet: Setup > Schnittstellen > WLAN

# lfc

Zeigt das Interface an, für das die Einstellungen der Adaptive RF Optimization gelten.

### SNMP-ID:

2.23.20.23.1

### Pfad Telnet:

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

# Aktiv

Aktiviert oder deaktiviert die Adaptive RF Optimization für diese Schnittstelle.

### SNMP-ID:

2.23.20.23.2

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

### Mögliche Werte:

nein ja

# **Default-Wert:**

nein

### **Min-Client-Phy-Signal**

Definieren Sie hier die minimale Signalstärke der Clients.

### SNMP-ID:

2.23.20.23.3

### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

### Mögliche Werte:

max. 3 Zeichen aus [0-9]

# **Default-Wert:**

15

### Min-Client-Tx-Pakete

Geben Sie hier die minimale Anzahl Pakete an, die an Clients gesendet werden soll.

### SNMP-ID:

2.23.20.23.4

### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

# Mögliche Werte:

max. 5 Zeichen aus [0-9]

### **Default-Wert:**

30

### **Tx-Client-Retry-Ratio-Limit**

Geben Sie in diesem Feld an, wie schnell ein Paket erneut an den Client übermittelt werden soll.

### 3 WLAN

#### SNMP-ID:

2.23.20.23.5

# Pfad Telnet:

 $Setup \ > Schnittstellen \ > WLAN \ > Adaptive-RF-Optimization$ 

# Mögliche Werte:

max. 3 Zeichen aus [0-9]

### Default-Wert:

70

# **Rauschpegel-Limit**

Definieren Sie die Obergrenze des Rauschpegels.

### SNMP-ID:

2.23.20.23.6

# **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

### Mögliche Werte:

max. 6 Zeichen aus [0-9]-

# **Default-Wert:**

-70

## Kanal-Markierung-Timeout

Legen Sie fest, wie lange der zur Zeit verwendete Kanal blockiert sein muss.

### SNMP-ID:

2.23.20.23.7

### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

# Mögliche Werte:

max. 5 Zeichen aus [0-9]

# **Default-Wert:**

20

### **Trigger-Zeitspanne**

Wählen Sie hier den minimalen Auslösezeitraum.

### SNMP-ID:

2.23.20.23.8

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Adaptive-RF-Optimization

### Mögliche Werte:

max. 5 Zeichen aus [0-9]

# Default-Wert:

1

# **3.2 Airtime Fairness**



Bessere WLAN-Performance durch effiziente Ausnutzung der zur Verfügung stehenden Bandbreite dank einer fairen Aufteilung der WLAN-Übertragungszeiten unter den aktiven Clients.

Insbesondere in WLAN-Szenarien mit einer hohen Dichte an Endgeräten konkurrieren die Clients um die zur Verfügung stehende Bandbreite. Dabei sendet der AP reihum an die aktiven Clients – ohne Berücksichtigung der notwendigen Übertragungszeit. So kommt es, dass langsamere (Legacy) Clients während der Übertragung von Datenpaketen schnellere Clients ausbremsen, obwohl diese in sehr kurzer Zeit ihre Datenübertragung abschließen könnten. Das Feature "Airtime Fairness" stellt sicher, dass die zur Verfügung stehende Bandbreite effizient ausgenutzt wird. Dazu wird die WLAN-Übertragungszeit ("Airtime") zwischen den aktiven Clients fair aufgeteilt. Die Folge: Dadurch, dass alle Clients dieselbe Airtime zur Verfügung haben, können schnellere Clients entsprechend mehr Datendurchsatz in derselben Zeit erreichen.

"Airtime" bedeutet WLAN-Übertragungszeit. Airtime Fairness stellt somit allen aktiven Clients eine WLAN-Übertragungszeit in Richtung der Clients entsprechend dem konfigurierten Airtime Fairness-Modus zur Verfügung. Dies verhindert z. B., dass ältere Clients moderne Clients ausbremsen.

Bei Geräten mit WLAN-Modulen, die den Standard IEEE 802.11ac unterstützen, ist die Funktion Airtime Fairness automatisch im WLAN-Modul aktiviert.

Folgende LANCOM-Geräte unterstützen Airtime Fairness: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

# 3.2.1 Airtime Fairness mit LANconfig konfigurieren

Wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt **Interfaces** auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie bei Geräten mit mehreren WLAN-Schnittstellen die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Performance**.

Physikalische WLAN-Einst WLAN-Interface 1	? 🔀
Betrieb Radio Adaptive RF Optimization Performance Client-Modus	
⊂ Super-A/G	
TX-Burst einschalten (Bündelung von WLAN-Paketen - nicht für 802.11n)	
Quality of Service	
🔲 QoS nach 802.11e (W/ME) einschalten	
Datenpakete mit der höchsten Priorität werden vor den niederprioren Paketen weitergeleitet. Bei ausgeschaltetem QoS wird die Paket-Priorisierung nicht berücksichtigt. Es erfolgt eine Gleichbehandlung der Pakete.	
Airtime Fairness	
Airtime Fairness-Modus: Gleiche Medienzeit 👻	
Der Standardwert 'gleiche Medienzeit' wird für die meisten Szenarien empfohle Änderung ist nur in Ausnahmefällen notwendig.	n. Eine
ОК	Abbrechen

Wählen Sie unter Airtime Fairness-Modus aus den verfügbaren Einstellmöglichkeiten die für Ihre WLAN-Umgebung passende Option aus:

### **Round-Robin-Verteilung**

Das Gerät sendet nacheinander an die aktiven Clients im Netzwerk.

### **Gleiche Medienzeit**

Alle Clients verfügen über die gleiche Airtime. Clients mit einer höheren Datenrate profitieren von dieser Einstellung, da sie in der gleichen Zeit mehr Daten empfangen können.



IEEE 802.11ac-fähige WLAN-Module verwenden bereits hardwareseitig einen Algorithmus, der dieser Einstellung entspricht.

### 802.11n bevorzugen

Diese Einstellung bevorzugt IEEE 802.11n-Clients gegenüber älteren Clients. Demnach erhalten Clients mit dem Standard 802.11a oder 802.11g im Verhältnis zum 802.11n lediglich 25% Airtime. Clients mit 802.11b-Standard erhalten nur 6,25% Airtime. Daher versendet das Gerät deutlich schneller Daten an Clients mit dem Standard IEEE 802.11n.

# **Gleiches Medienvolumen**

Diese Einstellung bewirkt, dass das Gerät die Airtime so zuweist, dass alle Clients die gleiche Datenmenge aus Richtung des APs erhalten. Allerdings bremsen langsamere Clients die schnelleren Teilnehmer bei dieser Option aus. Diese Einstellung ist nur sinnvoll, wenn ein gleicher Datendurchsatz bei allen Clients erforderlich ist.

# 3.2.2 Ergänzungen im Setup-Menü

 $(\mathbf{i})$ 

### Airtime-Fairness-Modus

Die Funktion **Airtime Fairness** optimiert die Übertragungsgeschwindigkeit, insbesondere in High-Density-Umgebungen, indem sie die verfügbare Bandbreite des WLANs gleichmäßig auf die Clients verteilt. In der Standardeinstellung ist **Airtime Fairness** aktiviert.

### SNMP-ID:

2.23.20.9.6

### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Leistung

### Mögliche Werte:

### **Round-Robin**

Jeder Client im Netzwerk erhält nacheinander eine Sendegelegenheit (TXOP).

### **Gleiche-Medienzeit**

Alle Clients verfügen über die gleiche Airtime. Clients mit einer höheren Datenrate profitieren von dieser Einstellung, da sie in der gleichen Zeit einen höheren Datendurchsatz erzielen können.

802.11ac-f\u00e4hige Ger\u00e4te verwenden bereits hardwareseitig einen Algorithmus, der dieser Einstellung entspricht.

### Bevorzuge-802.11n-Medienzeit

Diese Einstellung bevorzugt IEEE 802.11n-Clients gegenüber älteren Clients. Demnach erhalten Clients mit dem Standard 802.11a oder 802.11g im Verhältnis zum 802.11n lediglich 25% Airtime. Clients mit 802.11b-Standard erhalten nur 6,25% Airtime. Daher übertragen Clients mit dem Standard 802.11n ihre Daten wesentlich schneller.

#### **Gleiches-Volumen**

Erhalten alle Clients das gleiche Airtime-Kontingent, ist sichergestellt, dass jeder Client in der WLAN-Umgebung den gleichen Datendurchsatz erreicht. Allerdings bremsen langsamere Clients die schnelleren Teilnehmer bei dieser Option aus.



Diese Einstellung ist nur sinnvoll, wenn ein gleicher Datendurchsatz bei allen Clients erforderlich ist.

### **Default-Wert:**

Gleiche-Medienzeit

# 3.3 Verschlüsseltes OKC über IAPP

Ab LCOS-Version 9.18 RU1 besteht die Möglichkeit, OKC (Opportunistic Key Caching) auch in Netzwerken zu verwenden, in denen kein WLC eingesetzt wird.

# 3.3.1 Verschlüsseltes OKC über IAPP

OKC (Opportunistic Key Caching) ermöglicht es WLAN-Clients, Verbindungen zu APs aufzubauen, ohne sich bei jedem Aufbau komplett neu authentifizieren zu müssen. Wenn sich ein Client einmal mit einem AP verbunden und bei diesem authentifiziert hat, überträgt dieser AP den PMK (Pairwise Master Key) an einen WLC, der alle anderen APs im Netz darüber informiert. Somit ist der Client allen APs bekannt. Er handelt beim Wechsel in den Empfangsbereich eines benachbarten APs eine neue Verbindung aus und baut sie auf. Für diese Art OKC benötigt man jedoch einen WLC, der die Koordination der PMKs übernimmt.

Über das IAPP (Inter Access Point Protocol) tauschen APs im Netzwerk u. a. Informationen über verwendete BSSIDs und angemeldete WLAN-Clients aus. Somit ist es für einen Client möglich, sich zwischen den Empfangsbereichen verschiedener APs zu bewegen. Jeder AP fragt die Informationen des neuen Clients bei allen anderen APs an und teilt danach allen mit, dass der Client sich nun in seinem Bereich befindet. Diese Art der Kommunikation zwischen den APs lässt sich dafür nutzen, ein OKC direkt zwischen den APs und ohne WLC zu realisieren.

Durch eine definierte IAPP-Passphrase (PMK-IAPP-Secret) auf einem AP ist es möglich, den PMK (Pairwise Master Key) verschlüsselt zu den anderen APs zu übertragen und dort zu speichern. Somit steht OKC bei allen APs im Netz zur Verfügung, ohne dass ein WLC notwendig ist.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **802.11i/WEP** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.

E	WLAN-Verschlüsselungs-Einstell	ungen - Eintrag bearbeiten	? 💌						
	Allgemein Erweitert								
	WPA Rekeying-Zyklus:	0	Sekunden						
	WPA2 Key Management:	Standard 🗸							
	Client-EAP-Methode:	TLS -							
	IAPP-Passphrase:		Anzeigen						
		Passwort <u>e</u> rzeugen	]						
	PMK-Caching								
	Pre-Authentication								
	Authentifizierung:	Open-System (empfohlen) 🗢	]						
	Standardschlüssel:	Schlüssel 1 🔹 👻	]						
	Management-Frames verschlüsseln:	Nein 🔻	]						
L									
			OK Abbrechen						

# 3.3.2 Ergänzungen im Setup-Menü

# **PMK-IAPP-Secret**

Vernetzte APs tauschen Daten angemeldeter WLAN-Clients über das IAPP aus, um ein sicheres Roaming dieser WLAN-Clients zu ermöglichen. Der Mechanismus ist vergleichbar mit dem OKC mit WLC-Management, funktioniert jedoch komplett ohne WLCs.

Der AP nutzt diese Passphrase, um den PMK zu verschlüsseln und die Mobility Domain des jeweiligen WLAN-Clients zu errechnen.

Jeder Wert ungleich 0 startet automatisch den Austausch des Master Secrets zwischen den jeweiligen APs.

### SNMP-ID:

2.23.20.3.20

# Pfad Telnet:

```
Setup > Schnittstellen > WLAN > Verschluesselung
```

#### Mögliche Werte:

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

### **Default-Wert:**

leer

### **Besondere Werte:**

leer

OKC über IAPP ist deaktiviert.

# 3.4 Fast Roaming

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, Fast Roaming (IEEE 802.11r) auch in Netzwerken zu verwenden, in denen kein WLC eingesetzt wird.

# 3.4.1 Fast Roaming über IAPP

IEEE 802.11r verkürzt die Authentifizierung und reduziert somit Unterbrechungszeiten, die beim Übergang eines WLAN-Clients von einem AP zu einem anderen auftreten. Diese Unterbrechungszeiten können bei einigen hundert Millisekunden liegen.

Mit Fast Roaming über das Inter Access Point Protocol (IAPP) haben Sie die Möglichkeit, IEEE 802.11r direkt auf Ihren APs zu verwenden. Bislang war für diese Funktion ein WLC erforderlich.

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 APs mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **Verschlüsselung** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.

6	WLAN-Verschlüsselungs-Einstell	ungen - Eintrag bearbeiten		? <mark>- x</mark>
	Allgemein Erweitert			
	WPA Rekeving-Zyklus:	0	Sekunden	
	WPA2 Key Management:	Standard	•	
	Client-EAP-Methode:	TLS -	•	
	IAPP-Passphrase:		Anzeigen	
		Passwort <u>e</u> rzeugen	-	
	PMK-Caching			
	Pre-Authentication			
	Authentifizierung:	Open-System (empfohlen)	·	
	Standardschlüssel:	Schlüssel 1 🔹	·	
	Management-Frames verschlüsseln:	Nein	·	
				Abbrechen

() E

Beachten Sie bitte, dass es für die Verwendung von IEEE 802.11r erforderlich ist, in den Verschlüsselungs-Einstellungen unter **WPA2 Key Management** "Fast Roaming" auszuwählen.

# 3.4.2 Ergänzungen im Setup-Menü

# **PMK-IAPP-Secret**

Vernetzte APs tauschen Daten angemeldeter WLAN-Clients über das IAPP aus, um ein sicheres Roaming dieser WLAN-Clients zu ermöglichen. Der Mechanismus ist vergleichbar mit dem OKC mit WLC-Management, funktioniert jedoch komplett ohne WLCs.

Der AP nutzt diese Passphrase, um den PMK zu verschlüsseln und die Mobility Domain des jeweiligen WLAN-Clients zu errechnen.

Jeder Wert ungleich 0 startet automatisch den Austausch des Master Secrets zwischen den jeweiligen APs.

# SNMP-ID:

2.23.20.3.20

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Verschluesselung

### Mögliche Werte:

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

### Default-Wert:

leer

# Besondere Werte:

leer

OKC über IAPP ist deaktiviert.

# 3.5 Wireless Intrusion Detection System (WIDS)

Ein Intrusion Detection System (IDS) erkennt Angriffe auf ein Netzwerk und meldet diese Angriffe an ein übergeordnetes Netzwerk-Management-System. Gerade in Unternehmens-Netzwerken ist der Einsatz eines IDS unerlässlich, um eventuelle Angriffe oder Störungen sofort erkennen und abstellen zu können.

Das Wireless Intrusion Detection System (WIDS) in LCOS-Geräten überprüft die verfügbaren WLANs anhand umfangreicher, definierter Grenzwerte. Damit Sie im Falle eines Angriffes rechtzeitig reagieren können, meldet das WIDS Angriffe über E-Mail, SYSLOG oder SNMP-Traps.

Die Erkennung von Angriffen erfolgt dabei auf Basis von bekannten oder gleichartigen Mustern.

Beachten Sie bitte, dass die Erkennung von Angriffsmustern (Heuristik) auch zu Fehlalarmen ("False Positive") führen kann!

# 3.5.1 WIDS mit LANconfig konfigurieren

Um das Wireless Intrusion Detection System (WIDS) mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht Wireless-LAN > Security.

Wireless-IDS			
Mit dem Wireless Intrusion Detec Ihre Wireless-LAN-Infrastruktur e	ction System Irkennen.	(Wireless-IDS) könn	en Sie bestimmte Angriffe auf
🔲 Wireless-IDS aktiviert		Promisker Mo	odus
👿 Benachrichtigung via SYSLO	IG	Benachrichtig	gung via SNMP-Traps
Benachrichtigung via E-Mail	an		
E-Mail-Empfänger:			
E-Mail-Aggregat-Intervall:	10		Sekunden
Stellen Sie hier die Grenzwerte u Wireless-IDS ein. Diese Werte re	ınd Zeitinterv egeln, wann	alle der verschieden das Wireless-IDS Wa	en Alarm-Funktionen des arnungen generiert.
		Signaturen	]

### Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

### **Promisker Modus**

Bei aktiviertem Modus ("promiscuous mode") empfängt der AP auch Pakete, die nicht an ihn gerichtet sind, sondern an andere Netzwerkteilnehmer.

Dieser Modus ist erforderlich, um einige der unten genannten Angriffe erkennen zu können. Der promiscuous mode beeinflusst allerdings die Leistung. Daher wird mit der Aktivierung des promiscuous mode automatisch die Frame Aggregation abgeschaltet.

#### Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level "INFO" und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

### Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

### Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

**1** Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

### E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

Das Feld muss eine gültige E-Mail-Adresse enthalten.

### E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

# Signaturen

Hier konfigurieren Sie die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.

Signaturen					? 📑
Angriffs-Szenarien:			Mess-Intervall:		
EAPOL-Start:	250	Pakete	pro Intervall von:	10	Sekunden
Broadcast-Probe:	1.500	Pakete	pro Intervall von:	10	Sekunden
Authentication-Request:	250	Pakete	pro Intervall von:	10	Sekunden
Deauthentication-Request:	250	Pakete	pro Intervall von:	10	Sekunden
Broadcast-Deauthenticat.:	2	Pakete	pro Intervall von:	1	Sekunden
Association-Request:	250	Pakete	pro Intervall von:	10	Sekunden
Reassociation-Request:	250	Pakete	pro Intervall von:	10	Sekunden
Disassociation-Request:	250	Pakete	pro Intervall von:	10	Sekunden
Broadcast-Disassociate:	2	Pakete	pro Intervall von:	1	Sekunden
Out-Of-Window:	200	Pakete	pro Intervall von:	5	Sekunden
Block-Ack-after-DelBA:	100	Pakete	pro Intervall von:	5	Sekunden
Null-Data-Flood:	500	Pakete	pro Intervall von:	5	Sekunden
Null-Data-PS-Buffer-Overfl.:	200	Pakete	pro Intervall von:	5	Sekunden
Multi-Stream-Data:	100	Pakete	pro Intervall von:	5	Sekunden
Vorzeitiger EAPOL-Erfolg:	0	Pakete	pro Intervall von:	1	Sekunden
Vorzeitiger EAPOL-Fehler:	0	Pakete	pro Intervall von:	1	Sekunden
PS-Poll-TIM-Intervall:	100	Pakete	pro Intervall von:	5	Sekunden
Empfangs-Intervall-Diff.:	5				

Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (\*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (\*)
- Broadcast-Disassociate
- Out-Of-Window
- Block-Ack-after-DelBA
- Null-Data-Flood
- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data
- Vorzeitiger EAPOL-Erfolg (\*)
- Vorzeitiger EAPOL-Fehler (\*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

(\*) Diese Angriffe werden nur bei aktivem promiscuous mode erkannt!

# 3.5.2 Ergänzungen im Setup-Menü

# Wireless-IDS

In diesem Verzeichnis konfigurieren Sie das Wireless Intrusion Detection System (WIDS).

### SNMP-ID:

2.12.248

# Pfad Telnet:

Setup > WLAN

### **IDS-operational**

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

### SNMP-ID:

2.12.248.9

### Pfad Telnet:

Setup > WLAN > Wireless-IDS

### Mögliche Werte:

### nein

Das WIDS ist deaktiviert.

#### ja

Das WIDS ist aktiviert.

### **Default-Wert:**

nein

### Syslog-Operational

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level "INFO" und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Zugriffes und überschrittener Grenzwert).

### SNMP-ID:

2.12.248.10

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS

### Addendum

### 3 WLAN

### Mögliche Werte:

# nein

Die WIDS-Meldungen erfolgen nicht über SYSLOG.

# ja

Die WIDS-Meldungen erfolgen über SYSLOG.

# **Default-Wert:**

ja

# **SNMPTraps-Operational**

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

### SNMP-ID:

2.12.248.11

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS

# Mögliche Werte:

### nein

Die SNMP-Traps sind deaktiviert.

# ja

Die SNMP-Traps sind aktiviert.

# **Default-Wert:**

nein

# E-Mail

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

**1** Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

# SNMP-ID:

2.12.248.12

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS

### Mögliche Werte:

nein

Die WIDS-Meldungen über E-Mail sind deaktiviert.

# ja

Die WIDS-Meldungen erfolgen über E-Mail.

# **Default-Wert:**

nein

### E-Mail-Empfaenger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiv ist. Das Feld muss eine gültige E-Mail-Adresse enthalten.

### SNMP-ID:

2.12.248.13

# Pfad Telnet:

Setup > WLAN > Wireless-IDS

### Mögliche Werte:

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

### E-Mail-Zusammenfassungs-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

### SNMP-ID:

2.12.248.14

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

10

### Signaturen

In diesem Verzeichnis konfigurieren Sie die Grenzwerte und Zeitintervalle der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.

### SNMP-ID:

2.12.248.50

Pfad Telnet:

Setup > WLAN > Wireless-IDS

### AssociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Association-Request-Angriffe.

### SNMP-ID:

2.12.248.50.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Association-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

#### SNMP-ID:

2.12.248.50.1.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > AssociateReqFlood

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Association-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.1.2

### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > AssociateReqFlood

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

10

### ReassociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Reassociation-Request-Angriffe.

### SNMP-ID:

2.12.248.50.2

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Reassociation-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.2.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > ReassociateReqFlood

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Reassociation-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

#### SNMP-ID:

2.12.248.50.2.2

### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > ReassociateReqFlood

Addendum

3 WLAN

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

10

# AuthenticateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Authentication-Request-Angriffe.

### SNMP-ID:

2.12.248.50.3

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Authentication-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.3.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > AuthenticateReqFlood

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Authentication-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.3.2

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > AuthenticateReqFlood

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

**Default-Wert:** 

10

# EAPOLStart

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für EAPOL-Start-Angriffe.

### SNMP-ID:

2.12.248.50.4

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der EAPOL-Start-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.4.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > EAPOLStart

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die EAPOL-Start-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.4.2

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > EAPOLStart

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

10

3 WLAN

### ProbeBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Probe-Angriffe.

### SNMP-ID:

2.12.248.50.5

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Probe-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.5.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > ProbeBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

1500

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Probe-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.5.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > ProbeBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

10

### DisassociateBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Disassociate-Angriffe.

### SNMP-ID:

2.12.248.50.6

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Disassociate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.6.1

### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > DisassociateBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

2

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Disassociate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.6.2

### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > DisassociateBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### **Default-Wert:**

1

### DeauthenticateBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Deauthenticate-Angriffe.

### SNMP-ID:

2.12.248.50.7

3 WLAN

### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Deauthenticate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.7.1

### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > DeauthenticateBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

2

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Deauthenticate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

### SNMP-ID:

2.12.248.50.7.2

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > DeauthenticateBroadcast

### Mögliche Werte:

max. 4 Zeichen aus [0-9]

### Default-Wert:

1

### DisassociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Disassociation-Request-Angriffe.

### SNMP-ID:

2.12.248.50.8

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen
# Zaehlerlimit

Definieren Sie die Anzahl der Disassociation-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.8.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > DisassociateReqFlood

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Disassociation-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.8.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > DisassociateReqFlood

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

10

#### BlockAckOutOfWindow

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Out-Of-Window-Angriffe.

#### SNMP-ID:

2.12.248.50.9

# Pfad Telnet:

# Zaehlerlimit

Definieren Sie die Anzahl der Out-Of-Window-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

## SNMP-ID:

2.12.248.50.9.1

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > BlockAckOutOfWindow

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

200

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Out-Of-Window-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.9.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > BlockAckOutOfWindow

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

5

## BlockAckAfterDelBA

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Block-Ack-after-DelBA-Angriffe.

#### SNMP-ID:

2.12.248.50.10

# Pfad Telnet:

# Zaehlerlimit

Definieren Sie die Anzahl der Block-Ack-after-DelBA-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.10.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > BlockAckAfterDelBA

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

100

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Block-Ack-after-DelBA-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.10.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > BlockAckAfterDelBA

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

5

# NullDataFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Null-Data-Angriffe.

#### SNMP-ID:

2.12.248.50.11

# Pfad Telnet:

# Zaehlerlimit

Definieren Sie die Anzahl der Null-Data-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

#### SNMP-ID:

2.12.248.50.11.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > NullDataFlood

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

500

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Null-Data-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.11.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > NullDataFlood

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

5

## NullDataPSBufferOverflow

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Null-Data-PS-Buffer-Overflow-Angriffe.

#### SNMP-ID:

2.12.248.50.12

# Pfad Telnet:

# Zaehlerlimit

Definieren Sie die Anzahl der Null-Data-PS-Buffer-Overflow-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.12.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > NullDataPSBufferOverflow

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

200

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Null-Data-PS-Buffer-Overflow-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.12.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > NullDataPSBufferOverflow

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

#### **Default-Wert:**

5

# **PSPollTIMInterval**

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für PS-Poll-TIM-Intervall-Angriffe.

#### SNMP-ID:

2.12.248.50.13

# Pfad Telnet:

# Zaehlerlimit

Definieren Sie die Anzahl der PS-Poll-TIM-Intervall-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.13.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > PSPollTIMInterval

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

100

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die PS-Poll-TIM-Intervall-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.13.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > PSPollTIMInterval

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

5

# Intervall-Diff

## SNMP-ID:

2.12.248.50.13.3

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > PSPollTIMInterval

#### Mögliche Werte:

max. 4 Zeichen aus [0–9]

# **Default-Wert:**

5

#### SMPSMUltiStream

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Multi-Stream-Data-Angriffe.

#### SNMP-ID:

2.12.248.50.14

## **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Multi-Stream-Data-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

#### SNMP-ID:

2.12.248.50.14.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > SMPSMUltiStream

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

#### **Default-Wert:**

100

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Multi-Stream-Data-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.14.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > SMPSMUltiStream

## Mögliche Werte:

max. 4 Zeichen aus [0-9]

#### **Default-Wert:**

5

# DeauthenticateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Deauthentication-Request-Angriffe.

#### SNMP-ID:

2.12.248.50.15

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Deauthentication-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.15.1

#### **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > DeauthenticateReqFlood

## Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

250

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Deauthentication-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.15.2

#### Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > DeauthenticateReqFlood

# Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

10

# PrematureEAPOLSuccess

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Vorzeitiger-EAPOL-Erfolg-Angriffe.

# SNMP-ID:

2.12.248.50.16

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Zaehlerlimit

Definieren Sie die Anzahl der Vorzeitiger-EAPOL-Erfolg-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

#### SNMP-ID:

2.12.248.50.16.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > PrematureEAPOLSuccess

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# Default-Wert:

2

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Vorzeitiger-EAPOL-Erfolg-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.16.2

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > PrematureEAPOLSuccess

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

#### Default-Wert:

1

# PrematureEAPOLFailure

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Vorzeitiger-EAPOL-Fehler-Angriffe.

#### SNMP-ID:

2.12.248.50.17

# **Pfad Telnet:**

# Zaehlerlimit

Definieren Sie die Anzahl der Vorzeitiger-EAPOL-Fehler-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

## SNMP-ID:

2.12.248.50.17.1

# **Pfad Telnet:**

Setup > WLAN > Wireless-IDS > Signaturen > PrematureEAPOLFailure

## Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

2

# Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Vorzeitiger-EAPOL-Fehler-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

# SNMP-ID:

2.12.248.50.17.2

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen > PrematureEAPOLFailure

#### Mögliche Werte:

max. 4 Zeichen aus [0-9]

# **Default-Wert:**

1

## Promiscuous-Mode

Aktiviert oder deaktiviert den Promiscuous-Modus. Dieser Modus verarbeitet auch Pakete, die nicht an das Gerät selbst gesendet wurden. Diese Pakete werden an das LCOS weitergeleitet, um eine Analyse durch das WIDS zu ermöglichen.

Der Promiscuous-Modus erkennt folgende Angriffe:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess
- DeauthenticateReqFlood
- DisassociateReqFlood

Bitte beachten Sie, dass der Promiscuous-Modus die Leistung des Gerätes stark beeinträchtigt. So wird z. B. die Frame-Aggregation automatisch deaktiviert. Nutzen Sie diesen Modus daher nur bei konkretem Verdacht.

# SNMP-ID:

2.12.248.51

# Pfad Telnet:

Setup > WLAN > Wireless-IDS > Signaturen

# Mögliche Werte:

nein

Der Promiscuous-Modus ist deaktiviert.

ja

Der Promiscuous-Modus ist aktiviert.

# **Default-Wert:**

nein

# 3.6 Status-Zähler für fehlgeschlagene WPA-PSK / IEEE802.1X-Anmeldevorgänge

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, sich die Anzahl fehlgeschlagener Anmeldevorgänge für WPA und IEEE 802.1X anzeigen zu lassen.

# 3.6.1 Status-Zähler für WPA-PSK Anmeldevorgänge

Eine Übersicht über die Anzahl fehlgeschlagener WPA-PSK Anmeldevorgänge finden Sie im LCOS-Menübaum unter Status > WLAN > Verschlüsselung.

Zusätzlich erhalten Sie eine Übersicht über erfolgreiche Anmeldeversuche sowie die Anzahl zurückgewiesener Anmeldungen aufgrund falscher Passphrasen.

Verschluesselung													
Interface	Verschluesselung	Methode	WPA-Version	WPA1-Sitzungsschluesse	WPA2-Sitzungsschluesse	PMK-Caching	Prae-Authentisierung	окс	Gesch Mgmt-Frames	WPA2-Schluessel- Management	WPA-PSK- Anzahl- erfolgreich	WPA-PSK- Anzahl-Fehler	WPA-PSK-Anzahl- falsche-Passphrase
WLAN-1	ja	802.11i- WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-2	ja	802.11i- WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-3	ja	802.11i- WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-4	ja	802.11i- WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-5	ja	802.11i- WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-6	ja	802.11i-	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0

Wählen Sie in der Tabelle eine Schnittstelle aus (z. B. WLAN-1), um sich Informationen für die gewählte Schnittstelle anzeigen zu lassen.

Verschluesselung	
Verschluesselung Interface Verschluesselung Methode WPA-Version WPA1-Sitzungsschluessel WPA2-Sitzungsschluessel PMK-Caching Prae-Authentisierung OKC	WLAN-1 ja 802.11i-WPA-PSK WPA1/2 TKIP/AES TKIP/AES ja ja nein
GeschMgmt-Frames WPA2-Schluessel-Management WPA-PSK-Anzahl-erfolgreich WPA-PSK-Anzahl-Fehler WPA-PSK-Anzahl-falsche-Passphrase	nein Standard 0 0 9

# 3.6.2 Status-Zähler für IEEE 802.1X-Anmeldevorgänge

Eine Übersichtstabelle mit der Anzahl akzeptierter und zurückgewiesener Verbindungsanfragen je logischer Schnittstelle finden Sie im LCOS-Menübaum unter **Status** > **IEEE802.1x** > **Ports**.

Zusätzlich zeigt Ihnen die Übersicht an, wie oft bei einer Schnittstelle das Authorisierungslimit erreicht wurde.

Ports			
Port	Anzahl-Accept	Anzahl-Reject	Anzahl-ReauthMax-erreicht
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

# 3.6.3 Ergänzungen im Status-Menü

# WPA-PSK-Anzahl-falsche-Passphrase

Zeigt die Anzahl der zurückgewiesenen WPA-Anfragen aufgrund einer fehlerhaften Passphrase an dieser Schnittstelle an.

# SNMP-ID:

1.3.64.20

Pfad Telnet:

Status > WLAN > Verschlüsselung

# WPA-PSK-Anzahl-erfolgreich

Zeigt die Anzahl der erfolgreichen WPA-Anfragen an dieser Schnittstelle an.

#### SNMP-ID:

1.3.64.21

# Pfad Telnet:

Status > WLAN > Verschlüsselung

# WPA-PSK-Anzahl-Fehler

Zeigt die Anzahl der zurückgewiesenen WPA-Anfragen an dieser Schnittstelle an.

# SNMP-ID:

1.3.64.22

# Pfad Telnet:

Status > WLAN > Verschlüsselung

# Ports

In dieser Tabelle erhalten Sie eine Übersicht der angenommenen oder abgewiesenen Verbindungsanfragen je logischer Schnittstelle.

# SNMP-ID:

1.46.3

# **Pfad Telnet:**

Status > IEEE802.1x

# Port

Zeigt die Bezeichnung der Schnittstelle an.

# SNMP-ID:

1.46.3.1

# Pfad Telnet: Status > IEEE802.1x > Ports

#### Anzahl-Accept

Zeigt die Anzahl der erfolgreichen WPA-Anfragen an dieser Schnittstelle an.

# SNMP-ID:

1.46.3.2

# Pfad Telnet:

Status > IEEE802.1x > Ports

# Anzahl-Reject

Zeigt die Anzahl der zurückgewiesenen WPA-Anfragen an dieser Schnittstelle an.

#### SNMP-ID:

1.46.3.3

Pfad Telnet:

Status > IEEE802.1x > Ports

Anzahl-ReauthMax-erreicht

#### SNMP-ID:

1.46.3.4

# Pfad Telnet:

Status > IEEE802.1x > Ports

# 3.7 Adaptive Transmission Power

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, ausgefallene APs im Netzwerk durch Erhöhung der Sendeleistung weiterer APs automatisch auszugleichen.

# 3.7.1 Adaptive Transmission Power mit LANconfig konfigurieren

Die dynamische Sendeleistungsanpassung ist gerade für professionelle Backup-Szenarien in WLAN-Umgebungen unverzichtbar. Fällt ein AP aus, erhöhen die verbleibenden APs automatisch ihre Sendeleistung, sodass eine vollständige WLAN-Abdeckung zu jeder Zeit sichergestellt ist.

Geben Sie dazu an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden. Solange alle Geräte erreichbar sind, gilt für alle innerhalb dieser Gruppe befindlichen APs eine konfigurierbare Sendeleistungsreduktion (z. B. -6 dB). Dabei überprüfen die APs über das IAPP (Inter Access Point Protocol) ständig die korrekte Anzahl der APs im Netzwerk.

Fällt nun ein AP aus, ergibt die Überprüfung, dass die Anzahl der tatsächlich vorhandenen APs nicht der Anzahl der erwarteten APs entspricht, und die übrigen APs aktivieren die konfigurierte Rückfall-Sendeleistungs-Reduktion (z. B. 0 dB). Sobald der ausgefallene AP wieder erreichbar ist, entspricht bei der Überprüfung die tatsächliche Anzahl der APs der Anzahl der erwarteten Geräte. Die übrigen APs senken die Sendeleistung wieder auf den Standardwert. Für die Konfiguration wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **Allgemein**. Im Abschnitt "Erweiterte Einstellungen" klicken Sie auf die Schaltfläche **Experten WLAN-Einstellungen** und wählen ggf. bei APs mit mehreren WLAN-Schnittstellen die entsprechende Schnittstelle aus. Stellen Sie anschließend auf dem Reiter **Rückfall-Sendeleistungsreduktion** die Anzahl der erwarteten APs und die Rückfall-Sendeleistungs-Reduktion ein.

🔁 Experten WLAN-Einstellungen -	WLAN-Interface	? 🔀
Beaconing Roaming Rückfall-Ser	ndeleistungsreduktion	
Erwartete APs:	0	
Rückfall-SendeleistRed.	0	dB
		OK Abbrechen

# **Erwartete APs**

Geben Sie an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden.

#### Rückfall-Sendeleist.-Red.

Geben Sie hier die Sendeleistungs-Reduktion in dB an, die der AP nutzen soll, falls ein AP aus der konfigurierten Gruppe nicht mehr erreichbar sein sollte.



Die standardmäßige Sendeleistungs-Reduktion konfigurieren Sie unter **Wireless-LAN** > **Allgemein** mit der Schaltfläche **Physikalische WLAN-Einst.** (und ggf. Auswahl der WLAN-Schnittstelle) im Dialog unter **Radio**.

# 3.7.2 Ergänzungen im Setup-Menü

# **Redundanz-Einstellungen**

In diesem Verzeichnis konfigurieren Sie die dynamische Sendeleistungs-Anpassung beim Ausfall eines APs im Verbund mit mehreren APs.

#### SNMP-ID:

2.23.20.24

### Pfad Telnet:

Setup > Schnittstellen > WLAN

# lfc

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

#### SNMP-ID:

2.23.20.24.1

## Pfad Telnet:

Setup > Schnittstelle > WLAN > Redundanz-Einstellungen

#### Andere-APs-erwartet

Geben Sie hier die Anzahl der anderen APs an, die sich im AP-Verbund befinden.

Solange alle Geräte erreichbar sind, gilt für alle innerhalb dieser Gruppe befindlichen APs eine konfigurierbare Sendeleistungsreduktion (z. B. -6 dB). Dabei überprüfen die APs über das IAPP (Inter Access Point Protocol) ständig die korrekte Anzahl der APs im Netzwerk.

Fällt nun ein AP aus, ergibt die Überprüfung, dass die Anzahl der tatsächlich vorhandenen APs nicht der Anzahl der erwarteten APs entspricht, und die übrigen APs aktivieren die konfigurierte Rückfall-Sendeleistungs-Reduktion (z. B. 0 dB). Sobald der ausgefallene AP wieder erreichbar ist, entspricht bei der Überprüfung die tatsächliche Anzahl APs der Anzahl der erwarteten Geräte. Die übrigen APs senken die Sendeleistung wieder auf den Standardwert.

#### SNMP-ID:

2.23.20.24.2

## **Pfad Telnet:**

Setup > Schnittstelle > WLAN > Redundanz-Einstellungen

#### Mögliche Werte:

max. 5 Zeichen aus [0-9]

#### Backup-Sendeleistungs-Reduktion

Geben Sie hier die Sendeleistungs-Reduktion in dB an, die der AP nutzen soll, falls ein AP aus der konfigurierten Gruppe nicht mehr erreichbar sein sollte.

# SNMP-ID:

2.23.20.24.3

#### **Pfad Telnet:**

Setup > Schnittstelle > WLAN > Redundanz-Einstellungen

#### Mögliche Werte:

max. 3 Zeichen aus [0–9]

# 3.8 Erweiterte Startbedingungen für WLAN-RADIUS-Accounting

Im Normalfall sendet der WLAN-Stack eine RADIUS-Accounting-Start-Nachricht, sobald der WLAN-Client verbunden ist. Vielfach hat der WLAN-Client zu diesem Zeitpunkt noch keine IP-Adresse, weil sie u.U. vom DHCP-Server noch nicht zur Verfügung gestellt wurde. Das Attribut "Framed-IP-Address" innerhalb der RADIUS-Accounting-Nachricht kann somit nicht sinnvoll befüllt werden. Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, die Accounting-Start-Nachricht erst dann zu erzeugen, wenn der Client eine valide IP-Adresse erhalten hat. Somit erhält der RADIUS-Accounting-Server immer eine gültige Framed-IP-Address.

# 3.8.1 Startbedingungen für RADIUS-Accounting mit LANconfig konfigurieren

Wechseln Sie in LANconfig zu der Ansicht **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen**. Aktivieren Sie anschließend unter dem Reiter "Netzwerk" die Checkbox **RADIUS-Accounting aktiviert**.

Jetzt können Sie die Accounting-Start-Bedingungen über das Dropdown-Menü verändern. Dabei stehen Ihnen folgende Einstellungen zur Verfügung:

# Verbunden

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client in den Status "Verbunden" wechselt. Diese Einstellung ist als Standardwert definiert.

## Gültige IP-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IP-Adresse erhält (IPv4 oder IPv6).

#### Gültige IPv4-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv4-Adresse erhält.

## Gültige IPv6-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv6-Adresse erhält.

A

APIPA-Adressen (169.254.1.0 bis 169.254.254.255) werden nicht als gültige IP-Adressen anerkannt.

Logische WLAN-Einstellungen	- WLAN-Netzwerk 1		? ×					
Netzwerk Übertragung Alarme								
WLAN-Netzwerk aktiviert								
Netzwerk-Name (SSID):	PUBLICSPOT							
SSID-Broadcast unterdrücken:	Nein							
MAC-Filter aktiviert	W MAC-Filter aktiviert							
Maximalzahl der Clients:	0							
Minimale Client-Signal-Stärke:	0	%						
Client-Bridge-Unterstützung:	Nein	•]						
TX BandbrBegrenzung:	0	kbit/s						
RX BandbrBegrenzung:	0	kbit/s						
Client TX BandbrBegrenzung:	0	kbit/s						
Client RX BandbrBegrenzung:	0	kbit/s						
RADIUS-Accounting aktiviert								
RADIUS-Accounting-Server:	-	Wählen						
Accounting-Start-Bedingung:	Verbunden -							
LBS-Tracking aktiviert	Verbunden Gültige IP-Adresse							
LBS-Tracking-Liste:	Gültige IPv4-Adresse Gültige IPv6-Adresse							
Datenverkehr zulassen zwische								
U-)APSD / WMM-Powersave a								
I var Unicasis abeilagen, brueu- und multicasts unterdrücken								
		ОК	Abbrechen					

# **3.8.2 Startbedingungen für RADIUS-Accounting mit WEBconfig konfigurieren**

Wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk**. Hier haben Sie die Möglichkeit, die Accounting-Start-Bedingungen über das Dropdown-Menü zu verändern.

# 3.9 Auswahl eines RADIUS-Server-Profils bei Authentifizierung nach 802.1X

Ab LCOS-Version 9.18 RU1 steht Ihnen bei Verwendung einer Authentifizierung nach Standard IEEE 802.1X die Angabe eines RADIUS-Server-Profils zur Verfügung.

🔤 WLAN-Verschlüsselungs-Eins	tellungen - Eintrag bearbei	iten		? <mark>×</mark>
Allgemein Erweitert				
Interface:	Wireless Netzwerk 1			
Verschlüsselung aktivieren				
Methode/Schlüssel-1-Typ:	802.11i (WPA)-PSK	•		
Schlüssel 1/Passphrase:			Anzeigen	
	Passwort erzeugen	-		
RADIUS-Server:		Ŧ	Wählen	
WPA-Version:	WPA2	-		
WPA1 Sitzungsschlüssel-Typ:	TKIP	-		
WPA2 Sitzungsschlüssel-Typ:	AES			
			OK	Abbrechen

# **RADIUS-Server**

Wenn Sie unter **Methode/Schlüssel-1-Typ** eine Authentifizierung nach dem Standard IEEE 802.1X auswählen, geben Sie hier das Profil eines RADIUS-Servers an.

# 3.9.1 Ergänzungen im Setup-Menü

# **RADIUS-Profile**

Wenn Sie unter eine Authentifizierung nach dem Standard IEEE 802.1X verwenden, geben Sie hier das Profil eines RADIUS-Servers an.

# SNMP-ID:

2.23.20.3.21

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Verschlüsselung

# Mögliche Werte:

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

## **Default-Wert:**

leer

# 3.10 Konfigurierbare Datenraten pro WLAN-Modul

Ab LCOS-Version 9.18 RU1 ist es möglich, die Datenraten pro WLAN-Modul separat zu konfigurieren. Die folgenden LANCOM-Geräte unterstützen diese Möglichkeit:

- L-151
- L-3xx
- L-4xx
- L-822
- LN-830
- L-13xx
- IAP-xxx
- OAP-xxx
- Alle Geräte der E-Serie

Die aktuell genutzte Datenrate ist im Statusbaum am WLAN-Client und im LANmonitor sichtbar.

# 3.10.1 Konfigurierbare Datenraten je WLAN-Modul

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client "ankündigt", die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr.

() Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

# Konfiguration der Datenraten über LANconfig

Um die Datenraten mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** und öffnen Sie im Abschnitt **Erweiterte Einstellungen** den Dialog **WLAN-Übertragungsraten**. LANconfig listet die Einstellungen aller verfügbaren Schnittstellen auf. Um die Einstellung für eine Schnittstelle zu ändern, markieren Sie die entsprechende Schnittstelle und klicken Sie auf **Bearbeiten**.

Wählen Sie links den zu konfigurierenden Standard aus.

🔁 WLAN-Übertragungsraten - Eintrag I	pearbeiten				? <mark>×</mark>
802.11abg 802.11n HT-1 HT-2 HT-3 802.11ac	802.11 abg 1 Mbit: 2 Mbit: 5.5 Mbit: 11 Mbit: 6 Mbit: 9 Mbit:	Rx/Tx erforderlich     •       Rx/Tx erforderlich     •       Rx/Tx erforderlich     •       Rx/Tx erlaubt     •	12 Mbit: 18 Mbit: 24 Mbit: 36 Mbit: 48 Mbit: 54 Mbit:	Rx/Tx erlaubt       Rx/Tx erlaubt       Rx/Tx erlaubt       Rx/Tx erlaubt       Rx/Tx erlaubt       Rx/Tx erlaubt       Rx/Tx erlaubt	•
				ОК	Abbrechen

## Addendum

# 3 WLAN

🔁 WLAN-Übertragungsraten - Eintrag	bearbeiten			? 💌
802.11abg 802.11n HT-1 HT-2 HT-3 802.11ac	802.11n - HT-1- 6.5 Mbit: 19.5 Mbit: 39 Mbit: 58.5 Mbit:	Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼	13 Mbit: 26 Mbit: 52 Mbit: 65 Mbit:	Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼       Rx/Tx erlaubt     ▼
🕒 WLAN-Übertragungsraten - Eintrag	bearbeiten			OK Abbrechen
802.11abg 802.11n HT-1 HT-2 HT-3 802.11ac	802.11ac - VHT- MCS RX: 802.11ac - VHT- MCS RX: 802.11ac - VHT- MCS RX:	1 [Keine ▼] 2 [Keine ▼] 3 [Keine ▼]	MCS TX: MCS TX: MCS TX:	Keine   Keine  Keine
				OK Abbrechen

Die Konfiguration ist separat möglich für die Standards

- 802.11abg
- 802.11n
  - □ HT-1
  - □ HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Je nach Standard sind für jede Übertragungsrate je SSID und P2P-Strecke explizit die folgenden Einstellungen verfügbar:

# **Rx/Tx erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

## Rx/Tx erlaubt

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Rx erlaubt**

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Deaktiviert

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### MCS-9/8/7

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

#### Keine

Bei 802.11ac-Modulen ist die jeweilige Stream-Variante für die entsprechende Datenrichtung deaktiviert.

# 3.10.2 Ergänzungen im Setup-Menü

## Ratenauswahl

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client "ankündigt", die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr, was unter Umständen Airtime sparen kann.

Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

In diesem Verzeichnis konfigurieren Sie diese Datenraten.

#### SNMP-ID:

2.23.20.25

#### Pfad Telnet:

Setup > Schnittstellen > WLAN

#### 1M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.1

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx-erforderlich

# 2M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.2

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

# Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx-erforderlich

# lfc

Dieser Eintrag zeigt die zu konfigurierende Schnittstelle an.

#### SNMP-ID:

2.23.20.25.3

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# 5,5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

## SNMP-ID:

2.23.20.25.4

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

## Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

# 11M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.6

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

# 6M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.8

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

# nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# 9M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

# SNMP-ID:

2.23.20.25.9

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### 12M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.10

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# 18M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.11

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# 24M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.12

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

# Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Default-Wert:

Rx/Tx

# 36M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

# SNMP-ID:

2.23.20.25.13

# **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

# Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### 48M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.14

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Default-Wert:

Rx/Tx

# 54M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.15

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# HT-1-6.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.28

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Default-Wert:

Rx/Tx

#### HT-1-13M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.29

# **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

## Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

# HT-1-19.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.30

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

# HT-1-26M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.31

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

## nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# HT-1-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

# SNMP-ID:

2.23.20.25.32

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### HT-1-52M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.33

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# **Default-Wert:**

Rx/Tx

# HT-1-58.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.34

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

# **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

### HT-1-65M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.35

# Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

# **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

# Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

# Default-Wert:

Rx/Tx

# HT-2-13M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

# SNMP-ID:

2.23.20.25.36

# **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

# Mögliche Werte:

## nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.
### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

## Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

## HT-2-26M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.37

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## 3 WLAN

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

## HT-2-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.38

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### **Default-Wert:**

Rx/Tx

## HT-2-52M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.39

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Default-Wert:

Rx/Tx

## HT-2-78M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.40

## **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

## HT-2-104M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.41

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

## HT-2-117M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.142

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## **Default-Wert:**

Rx/Tx

## HT-2-130M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

## SNMP-ID:

2.23.20.25.43

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### HT-3-19.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.44

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

## HT-3-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.45

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### 3 WLAN

#### HT-3-58.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.46

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Default-Wert:

Rx/Tx

## HT-3-78M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.47

## **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

#### nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

## Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### **Default-Wert:**

Rx/Tx

#### HT-3-117M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.48

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## 3 WLAN

## Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Default-Wert:

Rx/Tx

## HT-3-156M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.49

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

## Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

#### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

### **Default-Wert:**

Rx/Tx

## HT-3-175.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.50

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

## **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

### **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

#### Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Default-Wert:

Rx/Tx

#### HT-3-195M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

#### SNMP-ID:

2.23.20.25.51

## **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

#### **Rx/Tx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

#### Rx/Tx

Der AP kündigt dem Client die Rate als "unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

## **Rx-erforderlich**

Der AP kündigt dem Client die Rate als "unterstützt" und "erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als "unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

## Default-Wert:

Rx/Tx

## VHT-1-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist f
ür die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS ausw
ählbar.

#### SNMP-ID:

2.23.20.25.105

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

#### Mögliche Werte:

None MCS7 MCS8 MCS9

## Default-Wert:

MCS9

## VHT-1-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.



Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

#### SNMP-ID:

2.23.20.25.106

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

Mögliche Werte:

None MCS7 MCS8 MCS9

#### **Default-Wert:**

MCS9

## VHT-2-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

## SNMP-ID:

2.23.20.25.115

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

Mögliche Werte:

None MCS7 MCS8 MCS9

**Default-Wert:** 

MCS9

#### VHT-2-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist f
ür die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS ausw
ählbar.

#### SNMP-ID:

2.23.20.25.116

Addendum

3 WLAN

#### **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

Mögliche Werte:

None MCS7 MCS8 MCS9

**Default-Wert:** 

MCS9

#### VHT-3-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.



Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

## SNMP-ID:

2.23.20.25.125

## **Pfad Telnet:**

Setup > Schnittstellen > WLAN > Ratenauswahl

Mögliche Werte:

None MCS7 MCS8 MCS9

#### **Default-Wert:**

MCS9

#### VHT-3-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

## SNMP-ID:

2.23.20.25.126

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Ratenauswahl

3 WLAN

Mögliche Werte:

None MCS7 MCS8 MCS9

Default-Wert:

MCS9

4 WLAN-Management

# 4 WLAN-Management

# 4.1 IAPP bei bestehendem CAPWAP-Tunnel automatisch abschalten

Ab LCOS-Version 9.18 RU1 deaktiviert ein WLC auf den verwalteten APs automatisch das IAPP, sobald ein CAPWAP-Verwaltungstunnel zwischen APs und WLC existiert.

# **5 LANCOM Location Based Services (LBS)**

# 5.1 Dynamische und persistente Tracking-Listen von WLAN Clients

Ab LCOS-Version 9.18 RU1 konfigurieren Sie die LBS-Tracking-Listen auch über LANconfig. Im WLC erfolgt die Konfiguration der LBS-Tracking-Liste über **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke**.

Logische WLAN-Netzwerke (SSIDs) - Neuer Eintrag				
📝 Logisches WLAN-Netzi	werk aktiviert	WPA-Version:	WPA2 -	]
Name:		WPA1 SitzungsschlTyp:	TKIP -	]
Vererbung		WPA2 SitzungsschlTyp:	AES -	]
Erbt Werte von Eintrag:	✓ Wählen	WPA2 Key Management:	Standard 🗸	]
-	Vererbte Werte	Basis-Geschwindigkeit:	2 Mbit/s 🗸	]
		Client-Bridge-Unterst.:	Nein 🗸	]
Netzwerk-Name (SSID):		TX BandbrBegrenzung:	0	kbit/s
SSID verbinden mit:	LAN am AP 🔹	RX BandbrBegrenzung:	0	kbit/s
VLAN-Betriebsart:	Untagged 🔹	Maximalzahl der Clients:	0	]
VLAN-ID:	2	Min. Client-Signal-Stärke:	0	%
Verschlüsselung:	802.11i (WPA)-PSK 🔻	EBS-Tracking aktiviert		
Schlüssel 1/Passphrase:	Anzeigen	LBS-Tracking-Liste:		]
	Passwort erzeugen 💌	📃 Lange Präambel bei 80	2.11b verwenden	
RADIUS-Profil:	DEFAULT - Wählen	U-)APSD / WMM-Pow	ersave aktiviert	
Zulässige FreqBänder:	2,4/5 GHz 🔹	MgmtFrames verschl.	Nein 🔻	J
Autarker Weiterbetrieb:	0 Minuten	802.11n		
802.11u-Netzwerk-Profil:	▼ Wählen	Max. Spatial-Streams:	Automatisch 🔹	]
OKC (Opportunistic Key Caching) aktiviert		V Kurzes Guard-Intervall zulassen		
MAC-Prüfung aktiviert		Frame-Aggregation verwenden     STBC (Space Time Block Coding) aktiviert		
SSID-Broad. unterdrücken: Nein 💌		Struct (Space Finite block Coulding) addreted Weither Could and the structure of		
RADIUS-Accounting ak	ktiviert zwischen Stationen dieser SSID			
Valenverkeni zulassen				
			ОК	Abbrechen

## **LBS-Tracking aktiviert**

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

## LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

#### 5 LANCOM Location Based Services (LBS)

Im AP erfolgt die Konfiguration der LBS-Tracking-Liste über Wireless-LAN > Allgemein > Logische WLAN-Einstellungen auf dem Tab Netzwerke.

😑 Logische WLAN-Einstellungen - WLAN-Interface 1 - Netzwerk 1 🛛 👘 💌				
Netzwerk Übertragung Alarme				
Interface:	WLAN-Interface 1 - Netzwerk 1			
WLAN-Netzwerk aktiviert	WLAN-Netzwerk aktiviert			
Netzwerk-Name (SSID):	LANCOM			
SSID-Broadcast unterdrücken:	Nein 👻	]		
MAC-Filter aktiviert				
Maximalzahl der Clients:	0	]		
Minimale Client-Signal-Stärke:	0	%		
Client-Bridge-Unterstützung:	Nein 🔻	]		
TX BandbrBegrenzung:	0	kbit/s		
RX BandbrBegrenzung:	0	kbit/s		
Client TX BandbrBegrenzung:	0	kbit/s		
Client RX BandbrBegrenzung:	0	kbit/s		
RADIUS-Accounting aktiviert				
RADIUS-Accounting-Server:		<u>W</u> ählen		
Accounting-Start-Bedingung:	Verbunden 👻	]		
LBS-Tracking aktiviert	LBS-Tracking aktiviert			
LBS-Tracking-Liste:		]		
☑ Datenverkehr zulassen zwischen Stationen dieser SSID				
U-)APSD / WMM-Powersave aktiviert				
Nur Unicasts ubettragen, Broad- und Multicasts unterdrucken				
		OK Abbrechen		

#### LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

## LBS-Tracking-Liste

**(i)** 

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

## 5.1.1 LBS-Tracking-Listen von Public-Spot-Benutzern verwenden

APs und WLCs bieten die Möglichkeit, angemeldete Public-Spot-Benutzer in Listen aufzunehmen und an einen LBS-Server (Location Based Service) zu melden.

Diese Funktion konfigurieren Sie für APs und WLCs im LANconfig unter **Public-Spot** > **Benutzer** im Abschnitt **LBS-Tracking**.

LBS-Tracking	
LBS-Tracking aktiviert	
LBS-Tracking-Liste:	

#### LBS-Tracking aktiviert

Bestimmen Sie hier, ob der LBS-Server die am Public Spot angemeldeten Benutzer nachverfolgen darf.

## LBS-Tracking-Liste

Name der LBS-Tracking-Liste, die der AP bzw. WLC an den LBS-Server sendet.

# 5.1.2 Ergänzungen im Setup-Menü

## LBS-Tracking

Bestimmen Sie hier, ob der LBS-Server die am Public Spot angemeldeten Benutzer nachverfolgen darf.

#### SNMP-ID:

2.24.38

## Pfad Telnet:

Setup > Public-Spot-Modul

## Mögliche Werte:

nein ja

#### Default-Wert:

nein

## LBS-Tracking-Liste

Name der LBS-Tracking-Liste

#### SNMP-ID:

2.24.39

#### **Pfad Telnet:**

Setup > Public-Spot-Modul

## Mögliche Werte:

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

#### **Default-Wert:**

leer

## LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

5 LANCOM Location Based Services (LBS)

#### SNMP-ID:

2.37.1.1.47

## Pfad Telnet:

Setup > WLAN-Management > AP-Konfiguration

## Mögliche Werte:

Name aus Setup > WLAN-Management > AP-Konfiguration > LBS-Tracking

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

## Default-Wert:

leer

## LBS-Tracking

Dieser Eintrag aktiviert oder deaktiviert das LBS-Tracking für diese SSID.

## SNMP-ID:

2.23.20.1.25

#### Pfad Telnet:

Setup > Schnittstellen > WLAN > Netzwerk

## Mögliche Werte:

nein

LBS-Tracking ist deaktiviert.

ja

LBS-Tracking ist aktiviert.

## LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

#### SNMP-ID:

2.23.20.1.26

## Pfad Telnet:

Setup > Schnittstellen > WLAN > Netzwerk

## Mögliche Werte:

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

#### Default-Wert:

leer

# **6 RADIUS**

# 6.1 Benutzerdefinierbare Attribute im RADIUS-Client

Ab LCOS-Version 9.18 RU1 haben Sie mit LANconfig die Möglichkeit, alle RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server eigenständig zu konfigurieren.

Unter LANconfig konfigurieren Sie die Attribute unter Kommunikation > RADIUS jeweils in den Abschnitten Authentifizierung über RADIUS für PPP und Clip und Tunnelauthentifizierung über RADIUS für L2TP.

Authentifizierung über RADIUS für PPP und CLIP			
RADIUS-Server: Deaktiviert	<ul> <li>Protokolle:</li> </ul>	RADIUS	
Adresse:			
Server Port:	1.812		
Absende-Adresse (optional):	-	Wählen	
Attributwerte:			
Schlüssel (Secret):		Anzeigen	
	Passwort erzeugen	]	
PPP-Arbeitsweise:	Deaktiviert 👻	]	
PPP-Authentifizierungs-Verfahren:			
PAP CHAP	MS-CHAP	MS-CHAPv2	
	Clip-Einstellungen		

Tunnelauthentifizierung über RADIUS für L2TP			
RADIUS-Server: Deaktiviert	<ul> <li>Protokolle:</li> </ul>	RADIUS	
Adresse:			
Port:	1.812		
Absende-Adresse (optional):	-	Wählen	
Attributwerte:			
Schlüssel (Secret):		Anzeigen	
	Passwort erzeugen		
Passwort:		Anzeigen	
	Passwort erzeugen		

#### Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form

```
<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>.
```

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- NAS-Port=1234 ist nicht erlaubt, da das Attribut nicht eindeutig ist (NAS-Port, NAS-Port-Id oder NAS-Port-Type).
- NAS-Id=ABCD ist erlaubt, da das Attribut eindeutig ist (NAS-Identifier).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben Service-Type=Framed und Service-Type=2 identisch.

Die Angabe eines Wertes in Anführungszeichen (" <Wert>") ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (\"), der umgekehrte Schrägstrich ebenfalls (\\).

Als Werte sind auch die folgenden Variablen erlaubt:

## %n

Gerätename

%**e** 

Seriennummer des Gerätes

88

Prozentzeichen

## %{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: Called-Station-Id=%{NAS-Identifier} setzt das Attribut Called-Station-Id auf den Wert, den das Attribut NAS-Identifier besitzt.

# 6.2 Zugriffsinformationen auf den RADIUS-Server automatisch bereinigen

Ab LCOS-Version 9.18 RU1 ist die Funktion "Auto-Loeschen-Accounting-Total" per Default aktiviert.

## 6.2.1 Ergänzungen im Setup-Menü

## Auto-Loeschen-Accounting-Total

Abgeschlossene Accouting-Sessions, deren RADIUS-Account von der Funktion "RADIUS-Nutzertabelle bereinigen" entfernt wurden, werden gelöscht.

#### SNMP-ID:

2.25.10.18

#### **Pfad Telnet:**

Setup > RADIUS > Server

## Mögliche Werte:

nein

Accounting-Informationen werden nicht automatisch gelöscht.

ja

Accounting-Informationen werden automatisch gelöscht.

## **Default-Wert:**

ja

# 6.3 Vendor Specific RADIUS-Attribut "LCS-Routing-Tag"

Ab LCOS-Version 9.18 RU1 unterstützt der RADIUS-Client für PPTP, L2TP und PPPoE das Vendor Specific Radius-Attribut "LCS-Routing-Tag".

# 7 Public Spot

# 7.1 Kürzere Einheiten für absolute Ablaufzeit

Ab LCOS-Version 9.18 RU1 ist es möglich, die Gültigkeit von Public Spot Vouchern mit kürzeren Zeiteinheiten (Tage, Stunden, Minuten) zu gestalten. Dies ist gerade in Szenarien mit hoher Kundenfrequenz bei gleichzeitig kurzer Verweildauer von Vorteil.

## 7.1.1 Kürzere Einheiten mit LANconfig konfigurieren

Um kürzere Ablaufzeiten für Public Spots mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Public-Spot** > **Assistent**. Wählen Sie anschließend im Abschnitt "Benutzer-Vorlage für E-Mail und SMS" im Dropdown-Menü die Einheit für den absoluten Ablauf aus. Passen Sie ggf. den Wert des absoluten Ablaufes an.

Benutzer-Vorlage für E-Mail und SMS			
elativ & absolut 🔹 🔻			
600	Sekunden		
5			
ige 🔹			
Mehifache Anmeldung			
	Anmeldungen		
	Minuten		
	Megabyte		
	lativ & absolut v 000 5 ge v		

# 7.2 Circuit-ID als Public Spot-URL-Redirect-Variable

Ab LCOS-Version 9.18 RU1 haben Sie mit der Redirect Variable "%d" die Möglichkeit, die Willkommensseite auf angemeldeten Clients je nach Standort zu verändern.

## 7.2.1 URL-Redirect Variable verwenden

Geben Sie den URL Parameter "%d" als Circuit ID an, z. B. http://ipaddress/?circuit=%d&nas=%i. Diese Variable ersetzt das Public Spot Modul mit der Circuit-ID, die im DHCP-Request des Clients erkannt wurde.

Dafür ist es erforderlich, dass auf dem AP "DHCP Snooping" so konfiguriert ist, dass der AP die Circuit ID in der Public Spot Stationstabelle des WLCs abfragen kann.

Somit ist es möglich, die Public Spot Willkommensseite auf den angemeldeten Clients je nach Standort zu verändern.

# 7.3 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, über die Web-API Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anzulegen.

## 7.3.1 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Bei Verwendung von Smart Ticket erhält der Benutzer im RADIUS-Server des lokalen Public Spot Gateways einen entsprechenden Public Spot Account.

Sind jedoch mehrere Public Spot Gateways im Einsatz und soll nur ein Gateway die Benutzerkonten in seinem RADIUS-Server vorhalten, wird der Public Spot Account bei der Verwendung von Smart Ticket auf dem zentralen RADIUS-Server angelegt. Dazu ist es notwendig, das entfernte Public Spot-Gateway im LCOS-Menübaum unter **Setup** > **Public-Spot-Modul** > **Authentifizierungs-Module** festzulegen.



Sofern kein entferntes Public Spot-Gateway definiert wird, werden Public Spot Benutzerkonten dem lokalen Public Spot-Gateway angelegt.

## 7.3.2 Ergänzungen im Setup-Menü

## **Radius-Server**

In diesem Menü nehmen Sie die Einstellungen zum Anlegen von Public Spot Benutzerkonten auf dem RADIUS-Server des entfernten Public-Spot-Gateways vor.

#### SNMP-ID:

2.24.41.5

#### Pfad Telnet:

Setup > Public-Spot-Modul > Authentifizierungs-Module

## Anbieter

Über diesen Eintrag definieren Sie das RADIUS-Server-Profil aus der Public Spot-Anbietertabelle, das den RADIUS-Server des entfernten Public-Spot-Gateways referenziert.

## SNMP-ID:

2.24.41.5.1

## **Pfad Telnet:**

Setup > Public-Spot-Modul > Authentifizierungs-Module > Radius-Server

## Mögliche Werte:

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

#### **Default-Wert:**

leer

## Name

Über diesen Eintrag definieren Sie, mit welchem Administratorkonto Benutzerkonten auf dem entfernten Public Spot-Gateway angelegt werden.

#### SNMP-ID:

2.24.41.5.2

#### Addendum

7 Public Spot

## Pfad Telnet:

```
Setup > Public-Spot-Modul > Authentifizierungs-Module > Radius-Server
```

## Mögliche Werte:

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

#### **Default-Wert:**

leer

## Passwort

Über diesen Eintrag definieren Sie das Passwort des oben angegebenen Administratorkontos.

#### SNMP-ID:

2.24.41.5.3

## Pfad Telnet:

Setup > Public-Spot-Modul > Authentifizierungs-Module > Radius-Server

#### Mögliche Werte:

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

#### Default-Wert:

leer

# 7.4 PMS-Template: AGBs akzeptieren

Die Anmeldung an einem Public Spot ist je nach Konfiguration abhängig davon, ob vorher die Nutzungsbedingungen zu bestätigen sind. Bei der Kombination verschiedener Anmeldemöglichkeiten (z. B. über gespeicherte Reservierungsdaten oder SMS-Authentifizierung) ist die Bestätigung der Nutzungsbedingungen bisher nicht klar zuzuordnen.

Ab LCOS-Version 9.18 RU1 wurde die Darstellung der Anmeldeseite bei Verwendung einer Kombination von Anmeldeverfahren überarbeitet.

# 7.5 Felder im Setup-Wizard "Public-Spot-Benutzer verwalten" ausblenden

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, Tabellenspalten im Assistenten "Public-Spot-Benutzer verwalten" dauerhaft auszublenden.

## 7.5.1 Felder mit WEBconfig ausblenden

Im Setup-Assistenten "Public-Spot-Benutzer verwalten" haben Sie über die Schaltfläche **Spalte zeigen/verstecken** die Möglichkeit, Tabellenspalten ein- oder auszublenden. Diese Änderungen sind jedoch nur temporär. Nach einem Seiten-Refresh oder bei einer neuen Sitzung werden die ausgeblendeten Spalten wieder angezeigt.

Um bestimmte Felder dauerhaft zu verbergen, wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**. Standardmäßig werden alle Felder angezeigt. Blenden Sie bestimmte Felder aus, um z. B. das Zeit-Budget zu verbergen, bleiben diese Spalten sowohl im Assistenten selbst als

auch im Dropdown-Menü unter der Schaltfläche **Spalte zeigen/verstecken** nach einem erneuten Aufrufen der Seite verborgen.

Um einen authentisierten Public Spot Benutzer zu löschen, müssen die Spalten "Rufende-Station-Id-Maske" und "Gerufene-Station-Id-Maske" im Assistenten sichtbar sein. Nicht authentisierte Benutzer hingegen lassen sich auch löschen, wenn beide Spalten ausgeblendet sind.

Beachten Sie bitte, dass ausgeblendete Felder beim Betätigen der Schaltfläche **Drucken** nicht mit ausgegeben werden. Die Ausgabe als CSV-Datei beinhaltet dagegen alle Daten. Sie haben jedoch die Möglichkeit, die Schaltfläche **Als CSV speichern** zu verbergen. Wechseln Sie dazu im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **CSV-Export-verstecken**. Wählen Sie "Ja" und speichern Sie Ihre Eingabe.

## Ergänzungen im Setup-Menü

#### Zeige-Ablauf-Typ

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Ablauf-Typ" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.12

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Ablauf-Typ" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Ablauf-Typ" aus.

#### **Default-Wert:**

ja

#### Zeige-Abs-Ablauf

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "absoluter Ablauf" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.13

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

#### Mögliche Werte:

## ja

Im Setup-Wizard wird die Spalte "absoluter Ablauf" angezeigt.

## nein

Der Setup-Wizard blendet die Spalte "absoluter Ablauf" aus.

7 Public Spot

### Default-Wert:

ja

## Zeige-Rel-Ablauf

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "relativer Ablauf" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.14

## Pfad Telnet:

## Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "relativer Ablauf" angezeigt. nein

Der Setup-Wizard blendet die Spalte "relativer Ablauf" aus.

## **Default-Wert:**

ja

## Zeige-Zeit-Budget

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Zeit-Budget" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.15

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

## ja

Im Setup-Wizard wird die Spalte "Zeit-Budget" angezeigt.

## nein

Der Setup-Wizard blendet die Spalte "Zeit-Budget" aus.

#### **Default-Wert:**

ja

## Zeige-Volumen-Budget

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Volumen-Budget-MByte" im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.16

#### **Pfad Telnet:**

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Volumen-Budget-MByte" angezeigt.

#### nein

Der Setup-Wizard blendet die Spalte "Volumen-Budget-MByte" aus.

#### **Default-Wert:**

ja

## Zeige-Case-Sensitiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Case-Sensitiv" im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.17

#### **Pfad Telnet:**

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Case-Sensitiv" angezeigt.

#### nein

Der Setup-Wizard blendet die Spalte "Case-Sensitiv" aus.

## **Default-Wert:**

ja

## Zeige-aktiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "aktiv" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.18

#### Addendum

7 Public Spot

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

## ja

Im Setup-Wizard wird die Spalte "aktiv" angezeigt.

#### nein

Der Setup-Wizard blendet die Spalte "aktiv" aus.

## **Default-Wert:**

ja

## Zeige-Tx-Limit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Tx-Limit" für die maximale Sende-Bandbreite im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.19

#### Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

#### ja

Im Setup-Wizard wird die Spalte "Tx-Limit" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Tx-Limit" aus.

#### **Default-Wert:**

ja

## Zeige-Rx-Limit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Rx-Limit" für die maximale Empfangs-Bandbreite im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.20

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## 7 Public Spot

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Rx-Limit" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Rx-Limit" aus.

## **Default-Wert:**

ja

### **Zeige-Rufende-Station**

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Rufende-Station-Id-Maske" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.21

## **Pfad Telnet:**

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

#### ja

Im Setup-Wizard wird die Spalte "Rufende-Station-Id-Maske" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Rufende-Station-Id-Maske" aus.

## **Default-Wert:**

ja

## **Zeige-Gerufene-Station**

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Gerufene-Station-Id-Maske" im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.22

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Gerufene-Station-Id-Maske" angezeigt.

7 Public Spot

nein

Der Setup-Wizard blendet die Spalte "Gerufene-Station-Id-Maske" aus.

## **Default-Wert:**

ja

## Zeige-Online-Zeit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Online-Zeit" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.23

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Online-Zeit" angezeigt.

#### nein

Der Setup-Wizard blendet die Spalte "Online-Zeit" aus.

## Default-Wert:

ja

## Zeige-Traffic

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Traffic (Rx / Tx Kbyte)" im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.24

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

## ja

Im Setup-Wizard wird die Spalte "Traffic (Rx / Tx Kbyte)" angezeigt.

#### nein

Der Setup-Wizard blendet die Spalte "Traffic (Rx / Tx Kbyte)" aus.

#### **Default-Wert:**

ja

## Zeige-Status-Spalte

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Status" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.25

## Pfad Telnet:

## Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Status" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Status" aus.

## **Default-Wert:**

ja

## Zeige-Mac-Adresse

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Mac-Adresse" im Setup-Wizard zu verbergen.

#### SNMP-ID:

2.24.44.26

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

## ja

Im Setup-Wizard wird die Spalte "Mac-Adresse" angezeigt.

## nein

Der Setup-Wizard blendet die Spalte "Mac-Adresse" aus.

#### **Default-Wert:**

ja

7 Public Spot

## Zeige-Ip-Adresse

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "IP-Adresse" im Setup-Wizard zu verbergen.

## SNMP-ID:

2.24.44.27

## Pfad Telnet:

Setup > Public-Spot-Modul > Verwalte-Benutzer-Assistent

## Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "IP-Adresse" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "IP-Adresse" aus.

## **Default-Wert:**

ja

# 7.6 Redirect für HTTPS-Verbindungen umschaltbar

Um die Last auf Public-Spot-Gateways gering zu halten, ist ab LCOS-Version 9.18 RU1 das Umleiten von HTTPS-Verbindungen unangemeldeter Clients wahlweise abschaltbar.

## 7.6.1 Redirect für HTTPS-Verbindungen

Versucht ein nicht angemeldeter Client über eine Schnittstelle, für die der Public Spot aktiv ist, via HTTPS auf eine Webseite zuzugreifen, wird diese Verbindungsanfrage an das Public Spot Gateway selber umgeleitet, um dem Nutzer die Anmeldeseite zu präsentieren. (Ist bei HTTP auch der Fall). In diesem Fall wird dem Benutzer normalerweise eine Zertifikatswarnung seines Browsers präsentiert, da der Name oder IP der ursprünglich angesurften Seite nicht der des Public Spot entspricht. Um dies und die Erzeugung von erhöhter Last durch die aufgebauten HTTPS-/TLS-Verbindungen auf dem Public Spot Gateway zu verhindern, kann mit dieser Einstellung der Verbindungsaufbau über HTTPS für unangemeldete Clients verhindert werden.

Ist der Client einmal angemeldet, findet keinerlei Umleitung mehr statt und es können beliebig HTTP- und HTTPS-Verbindungen durch den Client aufgebaut werden.

Heutzutage übliche Clients führen eine "Captive Portal Detection" via HTTP durch. Dabei wird versucht, auf eine bestimmte URL via HTTP zuzugreifen, um das Vorhandensein einer Anmeldeseite (durch Public Spot oder andere Lösungen) zu überprüfen. Dieser Mechanismus wird durch das Ausschalten der HTTPS-Umleitung nicht beeinflusst, da die Erkennung normalerweise über HTTP stattfindet.

Ist es in einem Public-Spot-Szenario jedoch nicht vorgesehen, dass unbekannte WLAN-Clients eine Verbindungsanfrage auch über HTTP ausführen sollen, würde dieser wirkungslose HTTPS-Redirect das Public-Spot-Gateway unnötig belasten. Entsprechend ist es möglich, diesen HTTPS-Redirect prinzipiell zu deaktivieren. In diesem Fall würde der Benutzer vom Browser eine leere Seite erhalten. Das Redirect für HTTPS-Verbindungen ist im LANconfig konfigurierbar unter **Public-Spot** > **Server** > **Betriebseinstellungen**.

Betriebseinstellungen		? 🗙	
Betriebseinstellungen			
Geben Sie an, für welche lokalen Netzwerk-Interfaces die Benutzer-Anmeldung aktiviert werden soll.			
	Interfaces	)	
Wählen Sie hier nur VLAN-IDs aus, wenn nicht alle Datenpakete über das entsprechende Interface geroutet werden sollen.			
	VLAN-Tabelle	]	
WEBconfig-Zugang über Public-Spot-Interface auf Authentifizierungsseiten einschränken			
Leerlaufzeitüberschreit.	0	Sekunden	
Geräte-Hostname:			
Der Public-Spot kann eine Gegenstelle überwachen und bei Ausfall der Internetverbindung den Benutzern eine temporäre Fehlerseite anzeigen.			
Gegenstelle:	-	Wählen	
TLS-Verbindungen von unauthentifizierten Clients annehmen			
	ОК	Abbrechen	

Aktivieren Sie die Option **TLS-Verbindungen von unauthentifizierten Clients annehmen**, um das HTTPS-Redirect einzuschalten. In der Standardeinstellung ist diese Option deaktiviert.

## 7.6.2 Ergänzungen im Setup-Menü

## **TLS-Verbindungen-umleiten**

Mit dieser Option bestimmen Sie, ob der Public Spot HTTPS-Verbindungen für unauthentifizierte Clients auf sich selber umleitet. Ist diese Option deaktiviert, können unauthentifizierte Clients keine HTTPS-Verbindungen aufbauen.

#### SNMP-ID:

2.24.51

## **Pfad Telnet:**

Setup > Public-Spot-Modul

## Mögliche Werte:

#### Nein

Der Public-Spot führt kein HTTPS-Redirect für nicht authentifizierte WLAN-Clients aus.

Ja

Der Public-Spot führt ein HTTPS-Redirect für nicht authentifizierte WLAN-Clients aus.

### **Default-Wert:**

Nein

# 7.7 Ausgabe des Bandbreitenprofils auf dem Voucher

Ab LCOS-Version 9.18 RU1 ist die Ausgabe des nutzerspezifischen Bandbreitenprofils auf dem Voucher möglich. Die Eingabe erfolgt im Voucher-Template in Form dieser neuen Vorlagen-Bezeichner:

## BANDWIDTHPROFNAME

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet das Bandbreiten-Profil, mit dem der Benutzer verknüpft ist.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

## RXBANDWIDTH

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet die maximale Empfangsbandbreite des Bandbreitenprofils.



Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

## TXBANDWIDTH

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet die maximale Sendebandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

# 7.8 Template-Vorschau

Ab LCOS-Version 9.18 RU1 haben Sie die Möglichkeit, sich eine Vorschau der hochgeladenen Public Spot Templates anzeigen zu lassen.
# 7.8.1 Template-Vorschau über WEBconfig

Um Änderungen an den Public Spot-Vorlagen verfolgen zu können, wechseln Sie in WEBconfig zur Ansicht **Extras** > **Public-Spot Template-Vorschau**.

Wählen Sie das anzuzeigende Template aus.
• 🕪 <u>Willkommensseite</u>
• 🕪 Login-Seite
• 🕪 <u>Fehlerseite</u>
• 🕪 <u>Startseite</u>
• 🕪 <u>Statusseite</u>
<ul> <li>Interpretation</li> <li>Interpretation<!--</td--></li></ul>
• 🕪 <u>Hilfeseite</u>
<ul> <li>Wein-Proxy-Seite</li> </ul>
<ul> <li>Voucher-Seite</li> </ul>
<ul> <li>Mutzungsbedingungen-Seite</li> </ul>
<ul> <li>Magistrierungs-Seite (E-Mail)</li> </ul>
<ul> <li>Maintender Maintender M Ander Maintender Ander Maintender Ander Maintender Ander Maintender Ander Maint Ander Maintender Maintender Maintender Maintender Maintender Maintender Maintender Ander Maintender Ander Mainten Ander Maint</li></ul>
<ul> <li>Megistrierungs-Seite (SMS)</li> </ul>
<ul> <li>Mathematical Annual Annua</li></ul>
<ul> <li>Mean Annual Annua</li></ul>

Wählen Sie ein Template zum Anzeigen aus der Liste aus.

Das ausgewählte Template wird im gleichen Browserfenster angezeigt. Über die "Zurück"-Funktion Ihres Browsers gelangen Sie zum WEBconfig zurück.

Einige Templates beinhalten einen Javascript-Code. Dieser Code wird beim Aufrufen des jeweiligen Templates ausgeführt. So enthält das Template "Voucher-Seite" z. B. den Code zum Ausdrucken, sobald die Seite angezeigt wird.

Auf dieser Seite sind Testdaten hinterlegt. Es wird jedoch kein entsprechender Benutzer angelegt. Sie haben also die Möglichkeit, das Template zu testen und auszudrucken.

rucken	22	ce895df7066a v ×
Drucker Name: Canon MP Status: Bereit Typ: Canon MP Standort: CNBJNP_I Kommentar:	1970 series Printer        970 series Printer       970 series Printer       0000085E765C6            Ausgabe in Datei	Test - WLAN Voucher Zugangsdaten / Access Data
Druckbereich	bis: 1 Dis: 1	(Hotspot
	SSID(Netzwerkname/Network name) Benutzername / Username: Passwort / Password: Gültig bis / Valid until: Dauer / Duration: Vorschau. Es wurde kein Benutzer an	: Test SSID Testuser Testpassword 01.01.2099 00:000 1 Stunde(n)/Hour(s) ngelegt.

 $\bigcirc$ 

Sofern kein Template vorliegt oder gefunden werden kann, erscheint eine Fehlermeldung im WEBconfig.

# 7.9 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Ab LCOS-Version 9.18 RU1 ist im Syslog die Dokumentation von DNS-Anfragen und -Antworten für die von Clients aufgerufenen Domains möglich.

```
7 Public Spot
```

# 7.9.1 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Der DNS-Server in LANCOM-Geräten löst DNS-Anfragen von Clients auf. Eine Übersicht darüber, welche Clients welche Namen angefragt haben und welche Antworten sie erhalten haben, steht im Syslog zur Verfügung.

Das Syslog des Routers/APs selbst kann nicht genutzt werden. Es ist daher erforderlich, einen externen Syslog-Server einzutragen.

Die Konfiguration des DNS-Loggings erfolgt im LANconfig unter IPv4 > DNS im Abschnitt SYSLOG.

SYSLOG			
DNS-Antworten an Clients könner	auf einem externen SYSLOG-Server protokolliert werden.		
V DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren			
Adresse des Servers:			
	Erweitert		

### DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Markieren Sie diese Option, um das DNS-Logging zu aktivieren.

Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter Meldungen > Allgemein im Abschnitt SYSLOG) erfolgt das DNS-Logging.

Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

PACKET\_INFO: DNS for <IP-Address>, TID {Hostname}: Ressource-Record

### **Adresse des Servers**

Enthält die IP-Adresse oder den DNS-Namen des zu nutzenden SYSLOG-Servers.

Die Einstellungen hinter der Schaltfläche Erweitert beeinflussen die Inhalte der SYSLOG-Meldungen.

Enweitert		? <mark>- x</mark>
Quelle:	Router 💌	
Priorität:	Notiz 👻	
Absende-Adresse (optional):	INTRANET -	Wählen
	OK	Abbrechen

#### Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

# Priorität

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

### Absende-Adresse (optional)

Enthält die Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

# 7.9.2 Ergänzungen im Setup-Menü

# Syslog

In diesem Verzeichnis konfigurieren Sie die Ausgabe von DNS-Anfragen und -Antworten im Syslog für von Clients aufgerufene Domains.

SNMP-ID:

2.17.20

Pfad Telnet:

Setup > DNS

## DNS-Aufloesungen-loggen

Aktiviert bzw. deaktiviert die Aufzeichnung von DNS-Anfragen und -Antworten.

Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter Setup > SYSLOG > Aktiv auf "Nein") erfolgt das DNS-Logging.

Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

PACKET\_INFO: DNS for <IP-Address>, TID {Hostname}: Ressource-Record

#### SNMP-ID:

2.17.20.1

Pfad Telnet:

Setup > DNS > Syslog

# Mögliche Werte:

#### nein

Deaktiviert die Aufzeichnung der DNS-Anfragen.

ja

Aktiviert die Aufzeichnung der DNS-Anfragen.

### **Default-Wert:**

nein

### Log-Server-Adresse

Die Log-Server-Adresse enthält den zu nutzenden Syslog-Server in Form des entsprechenden DNS-Namens oder einer IP-Adresse.

Die IP-Adressen 127.0.0.1 und :: 1 werden generell abgelehnt, um so die Nutzung eines externen Servers zu erzwingen.

### SNMP-ID:

2.17.20.2

# Pfad Telnet:

Setup > DNS > Syslog

### Mögliche Werte:

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

### Addendum

7 Public Spot

# Log-Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

# SNMP-ID:

2.17.20.3

# Pfad Telnet:

Setup > DNS > Syslog

# Mögliche Werte:

System Login Systemzeit Konsole-Login Verbindungen Accounting Administration Router

# **Default-Wert:**

Router

# Log-Level

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

# SNMP-ID:

2.17.20.4

# **Pfad Telnet:**

Setup > DNS > Syslog

# Mögliche Werte:

Notfall Alarm Kritisch Fehler Warnung Hinweis Info Debug

# **Default-Wert:**

Hinweis

### Loopback-Addr.

Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

### SNMP-ID:

2.17.20.5

# Pfad Telnet:

Setup > DNS > Syslog

# Mögliche Werte:

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

# **Besondere Werte:**

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll "INT" für die Adresse des ersten Intranets "DMZ" für die Adresse der ersten DMZ LB0 bis LBF für die 16 Loopback-Adressen Beliebige gültige IP-Adresse

# Facility

Zuordnung der Quellen zu bestimmten Facilities.

### SNMP-ID:

2.22.3.2

Pfad Telnet:

Setup > SYSLOG > Facility-Mapper

7 Public Spot

Mögliche Werte:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

# **IP-Adresse**

Zuordnung der IP-Adresse zu bestimmten Facilities.

# SNMP-ID:

2.22.2.7

# **Pfad Telnet:**

Setup > SYSLOG > Tabelle-SYSLOG

### Mögliche Werte:

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

# 7.10 Schutz vor Brute Force-Angriffen

Ab Version 9.18 RU1 bietet LCOS Schutz vor Brute Force-Angriffen im Public Spot.

# 7.10.1 Schutz vor Brute Force-Angriffen

Brute-Force-Angriffe sind die bekanntesten Angriffe auf ein Netzwerk. Diese Art von Angriff besteht darin, eine Menge an möglichen Passwörter innerhalb kurzer Zeit auszuprobieren, bis das richtige Passwort gefunden wird. Ein möglicher

Schutz vor Brute-Force-Angriffen besteht darin, nach einem oder mehreren aufeinander folgenden fehlgeschlagenen Eingabeversuchen die Zeit bis zur nächsten möglichen Eingabe zu verzögern.

Den Schutz vor Brute-Force-Angriffen konfigurieren Sie mit LANconfig unter **Public-Spot** > **Server** im Abschnitt **Brute-Force-Schutz**.

Brute-Force-Schutz		
Sperren nach:	10	Fehlversuchen
Sperrdauer:	60	Minuten

### Sperren nach

Bestimmen Sie, nach wievielen Fehlversuchen die Eingabesperre für weitere Versuche eingreifen soll.

### Sperrdauer

Bestimmen Sie, für wie lange die Eingabesperre gelten soll.

Über die Konsole zeigt der Befehl show pbbruteprotector den aktuellen Status des Brute-Force-Schutzes:

### show pbbruteprotector

Zeigt eine Übersicht über alle am Public-Spot angemeldeten MAC-Adressen.

# show pbbruteprotector [MAC-Adresse[ MAC-Adresse[ ...]]]

Die Angabe einer oder mehrerer durch Leerzeichen getrennte MAC-Adressen zeigt den Status der jeweiligen MAC-Adressen an.



Die Angabe der MAC-Adresse erfolgt in den Formaten 11:22:33:44:55:66, 11-22-33-44-55-66 oder 112233445566.

# 7.10.2 Ergänzungen im Setup-Menü

# **Brute-Force-Schutz**

Dieses Menu enthält die Einstellungen für den Brute-Force-Schutz des Public-Spots.

#### SNMP-ID:

2.24.49

# Pfad Telnet:

Setup > Public-Spot-Modul

# Max-Login-Versuche

Bestimmen Sie, nach wievielen Fehlversuchen die Loginsperre für weitere Versuche eingreifen soll.

#### SNMP-ID:

2.24.49.1

### Pfad Telnet:

Setup > Public-Spot-Module > Brute-Force-Schutz

### Addendum

7 Public Spot

### Mögliche Werte:

max. 3 Zeichen aus [0-9]

# Default-Wert:

10

# Sperrzeit-In-Minuten

Bestimmen Sie, für wie lange die Loginsperre des Brute-Force-Schutzes gelten soll.

### SNMP-ID:

2.24.49.2

# Pfad Telnet:

Setup > Public-Spot-Modul > Brute-Force-Schutz

### Mögliche Werte:

max. 5 Zeichen aus [0-9]

# **Default-Wert:**

60

### **Entsperren-Check-In-Sekunden**

Bestimmen Sie, in welchem Abstand der AP den Ablauf einer Loginsperre für eine MAC-Adresse prüft.

#### SNMP-ID:

2.24.49.3

# **Pfad Telnet:**

Setup > Public-Spot-Modul > Brute-Force-Schutz

### Mögliche Werte:

max. 5 Zeichen aus [0-9]

### **Default-Wert:**

60

# Entsperren

Mit dieser Aktion entfernen Sie die Loginsperre für eine MAC-Adresse. Geben Sie als Parameter eine oder mehrere durch Leerzeichen getrennte MAC-Adressen ein.



Die Angabe der MAC-Adresse erfolgt in den Formaten 11:22:33:44:55:66, 11–22–33–44–55–66 oder 112233445566.

7 Public Spot

# SNMP-ID:

2.24.49.4

# Pfad Telnet:

 $Setup \ > Public-Spot-Modul \ > Brute-Force-Schutz$ 

# 8 Routing und WAN-Verbindungen

# 8.1 Route-Monitor

Ab LCOS-Version 9.18 RU1 überprüft ein Route-Monitor die Netzwerk-Verbindungen zu einem definierten Präfix. Dieses gelernte Präfix ist z. B. das Ergebnis eines dynamischen Routing-Protokolls wie BGP.

Bei einer fehlerhaften Verbindung startet der Route-Monitor ggf. eine Backup-Verbindung.

# 8.1.1 Route-Monitor

Der Route-Monitor überwacht Verbindungen zu Netzwerken verschiedener Provider und stellt im Fehlerfall eine Backup-Verbindung her. Die Überwachung geschieht über ein Trigger-Präfix, das der Provider in seinem Routing-Protokoll zur Verfügung stellt, z. B. beim Border Gateway Protokoll (BGP). Sobald die Route zu einem Provider-Netzwerk unerreichbar ist, erklärt der Route-Monitor das entsprechende Trigger-Präfix im eigenen Netzwerk für ungültig und öffnet eine Backup-Verbindung zum Provider-Netzwerk.

In LANconfig konfigurieren Sie Route-Monitor unter Kommunikation > Ruf-Verwaltung.

	Backup-Ta	belle	
Backup-Verbindung nach:	30	Sekunden	
Geben Sie die Zahl der Rückruf	fe bei Verbindungen mit	automatischem Rückruf an.	
Rücknif-Versuche:	3		
Dente Manharalationa			
Route-Monitor aktiviert In dieser Tabelle kann das Vorhigter	andensein von Präfixer	n in der Routing-Tabelle überwacht w	erden
Route-Monitor aktivient in dieser Tabelle kann das Vorh und ggf. eine Backup-Verbindu	andensein von Präfixe ng aufgebaut werden.	n in der Routing-Tabelle überwacht w	erden

Aktivieren Sie die Checkbox **Route-Monitor aktiviert**. Klicken Sie anschließend auf die Schaltfläche **Route-Monitor-Tabelle**.

R	Route-Monitor-Tabelle - Neuer Eintrag			
	📝 Aktiv			
	Gegenstelle:	DEFAULT -	Wählen	
	Präfix:			
	Routing-Tag:	0		
l	Aktivierungsverzögerung:	20	Sekunden	
	Deaktivierungsverzögerung:	0	Sekunden	
ł.	Kommentar:			
		OK	Abbrechen	

Fügen Sie der Tabelle einen neuen Eintrag hinzu und aktivieren Sie die Checkbox **Aktiv**, falls Sie diese Backup-Verbindung aktivieren möchten.

Definieren Sie folgende Parameter:

### Gegenstelle

Enthält den Namen der Backup-Gegenstelle.

### Präfix

Enthält das Präfix (IPv4- oder IPv6-Adresse), das der Route-Monitor überwachen soll.

# **Routing-Tag**

Enthält das Routing-Tag des zu überwachenden Präfixes.

### Aktivierungsverzögerung

Enthält die Verzögerung in Sekunden, die das Gerät nach dem Ausbleiben des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle aufbaut.

## Deaktivierungsverzögerung

Definiert die Verzögerung in Sekunden, die das Gerät nach dem Auftauchen des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle wieder abbaut.

### Kommentar

Enthält einen Kommentar zu diesem Eintrag.

# 8.1.2 Ergänzungen im Setup-Menü

## **Route-Monitor**

In diesem Verzeichnis konfigurieren Sie den Route-Monitor.

### SNMP-ID:

2.93.2

### Pfad Telnet:

Setup > Routing-Protokolle

# **Monitor-Tabelle**

In dieser Tabelle konfigurieren Sie den Route-Monitor.

### SNMP-ID:

2.93.2.1

### **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor

### **Backup-Gegenstelle**

Enthält den Namen der Backup-Gegenstelle.

8 Routing und WAN-Verbindungen

#### SNMP-ID:

2.93.2.1.1

# Pfad Telnet:

### Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

# Mögliche Werte:

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

### **Default-Wert:**

leer

# Praefix

Enthält das Präfix (IPv4- oder IPv6-Adresse), das der Route-Monitor überwachen soll.

### SNMP-ID:

2.93.2.1.2

# **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

### Mögliche Werte:

```
max. 43 Zeichen aus [A-F][a-f][0-9]:./
```

### **Default-Wert:**

leer

# Rtg-Tag

Enthält das Routing-Tag des zu überwachenden Präfixes.

### SNMP-ID:

2.93.2.1.3

### **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

### Mögliche Werte:

max. 5 Zeichen aus [0-9]

# **Default-Wert:**

0

### Aktivierungsverzoegerung

Enthält die Verzögerung in Sekunden, die das Gerät nach dem Ausbleiben des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle aufbaut.

### SNMP-ID:

2.93.2.1.4

### **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

### Mögliche Werte:

max. 10 Zeichen aus [0-9]

#### **Default-Wert:**

20

### Deaktivierungsverzoegerung

Definiert die Verzögerung in Sekunden, die das Gerät nach dem Auftauchen des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle wieder abbaut.

### SNMP-ID:

2.93.2.1.5

#### Pfad Telnet:

### Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

### Mögliche Werte:

max. 10 Zeichen aus [0-9]

### **Default-Wert:**

0

### **Besondere Werte:**

### 0

Keine Verzögerung: Das Gerät beendet die Verbindung zur Backup-Gegenstelle sofort beim Auftauchen des Präfixes.

#### Aktiv

Gibt an, ob diese Backup-Verbindung aktiv ist.

### SNMP-ID:

2.93.2.1.6

#### **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

8 Routing und WAN-Verbindungen

### Mögliche Werte:

Ja

Die Backup-Verbindung ist aktiv.

Nein

Die Backup-Verbindung ist nicht aktiv.

# **Default-Wert:**

Nein

# Kommentar

Kommentar zu diesem Eintrag.

# SNMP-ID:

2.93.2.1.7

# **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor > Monitor-Tabelle

### Mögliche Werte:

max. 254 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()+-,/:;<=>?[\]^\_.`

## **Default-Wert:**

leer

# Aktiv

Mit dieser Aktion aktivieren oder deaktivieren Sie den Route-Monitor.

### SNMP-ID:

2.93.2.2

### **Pfad Telnet:**

Setup > Routing-Protokolle > Route-Monitor

### Mögliche Werte:

## nein

Der Route-Monitor ist deaktiviert.

# ja

Der Route-Monitor ist aktiviert.

# **Default-Wert:**

nein

# 8.2 DiffServ-Feld per Default aktiviert

Ab LCOS-Version 9.18 RU1 beachtet die Routing-Methode im LCOS-Menübaum unter **Setup** > **IP-Router** > **Routing-Methode** standardmäßig das DiffServ-Feld. Somit ist als Routing-Methode per Default DiffServ aktiviert.

# 8.2.1 Ergänzungen im Setup-Menü

# **Routing-Methode**

Bestimmt die Auswertung der ToS- oder DiffServ-Felder.

### SNMP-ID:

2.8.7.1

### **Pfad Telnet:**

Setup > IP-Router > Routing-Methode

# Mögliche Werte:

## Normal

Das ToS/DiffServ-Feld wird ignoriert.

#### TOS

Das ToS/DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits "Low-Delay" und "High-Reliability" ausgewertet.

### DiffServ

Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

- CSx (inklusive CS0 = BE): normal übertragen
- AFxx: gesichert übertragen
- EF: bevorzugt übertragen

# **Default-Wert:**

DiffServ

# 9 Weitere Dienste

Ein Gerät bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzen mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Bürokommunikations-Funktionen mit LANCAPI
- Zeit-Server

# 9.1 IPv6-Unterstützung durch (S)NTP-Client und -Server

LCOS-Version 9.18 RU1 unterstützt IPv6 für den (S)NTP-Client und -Server.