connecting your business

Addendum

LCOS 9.18

LANCOM Systems

Inhalt

1 Addendum zur LCOS-Version 9.18....3
2 WLAN....4
2.1 Adaptive RF Optimization....4
2.1.1 Adaptive RF Optimization mit LANconfig konfigurieren....5
2.2 Airtime Fairness....6
2.2.1 Airtime Fairness mit LANconfig konfigurieren....7
2.3 Wireless Intrusion Detection System (WIDS)....8
2.3.1 WIDS mit LANconfig konfigurieren....8
3 Ergänzungen im Menüsystem....11
3.1 Ergänzungen im Setup-Menü....11
3.1.1 Wireless-IDS....11
3.1.2 Airtime-Fairness-Modus....31
3.1.3 Adaptive-RF-Optimization....32
3.2 Ergänzungen im Status-Menü....35
3.2.1 Powersave-Wiederholungen....35
3.2.2 Adaptive-RF-Optimization....35
3.2.3 Wireless-IDS....35

1 Addendum zur LCOS-Version 9.18

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

Änderungen am LCOS-Menübaum finden Sie im Abschnitt *Ergänzungen im Menüsystem* dieses Addendums.

2 WLAN

2.1 Adaptive RF Optimization

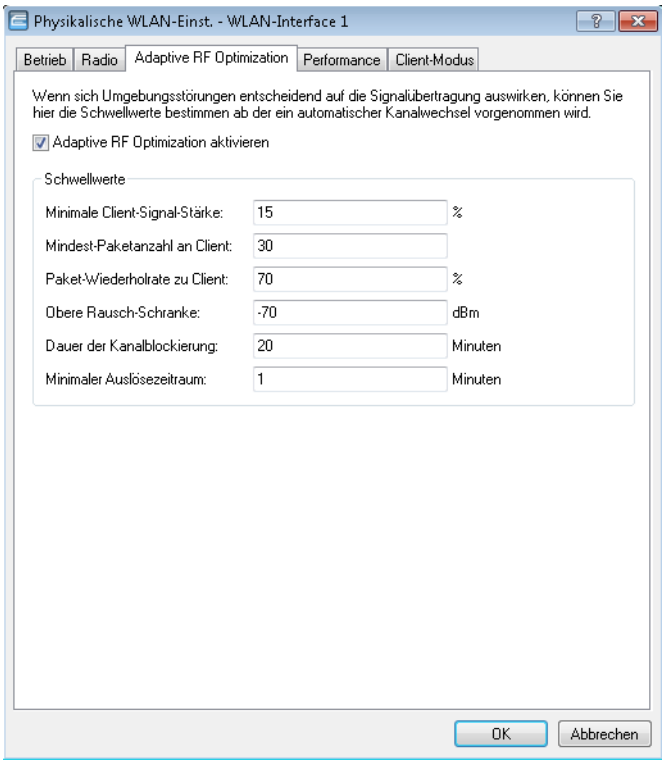
Höherer WLAN-Durchsatz im Funkfeld dank dynamischer Auswahl des qualitativ besten WLAN-Kanals durch den Access Point bei Kanalstörungen.

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 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.

2.1.1 Adaptive RF Optimization mit LANconfig konfigurieren

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 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 TX-Pakete mindestens an einen Client gesendet werden müssen. 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.

2.2 Airtime Fairness

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

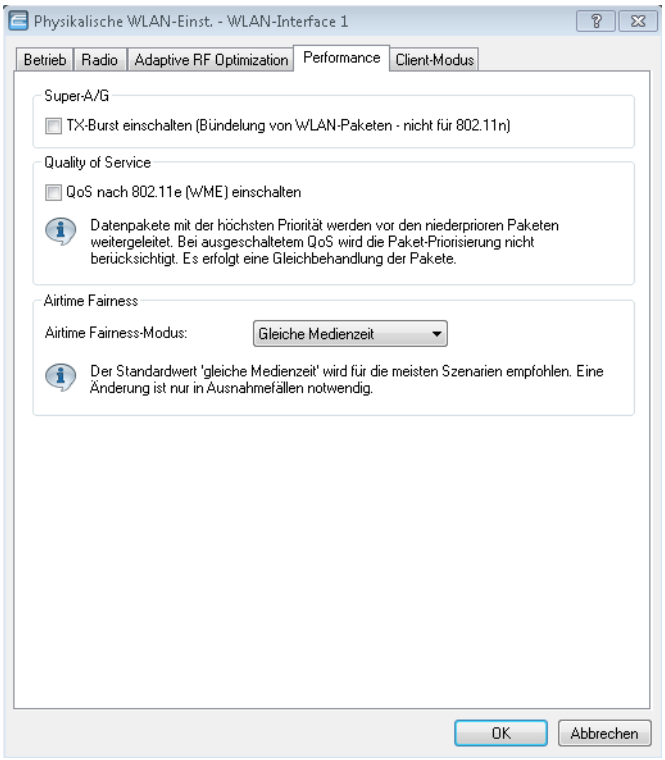
Insbesondere in WLAN-Szenarien mit einer hohen Dichte an Endgeräten konkurrieren die Clients um die zur Verfügung stehende Bandbreite. Dabei sendet der AP reihum an die aktiven Clients – ohne Berücksichtigung der notwendigen Übertragungszeit. So kommt es, dass langsamere (Legacy) Clients während der 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 werden die WLAN-Übertragungszeiten („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.

2.2.1 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**.



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 nach 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.

2.3 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.

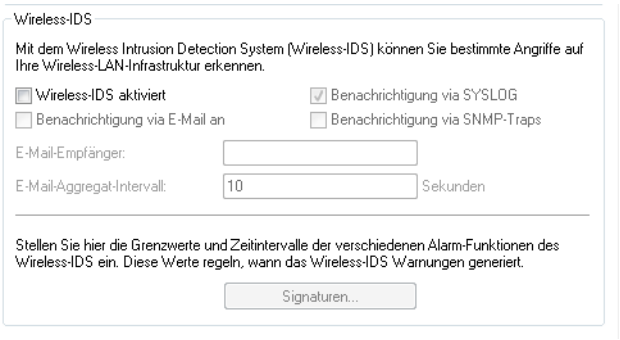
Das Wireless Intrusion Detection System (WIDS) in LCOS-Geräten überprüft die verfügbaren WLANs anhand umfangreicher, definierter Grenzwerte. Damit Sie im Falle eines Angriffes rechtzeitig reagieren können, meldet das WIDS Angriffe über E-Mail, SYSLOG oder SNMP-Traps.

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!

2.3.1 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 aktiviert

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

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 Zugriffes 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.

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.

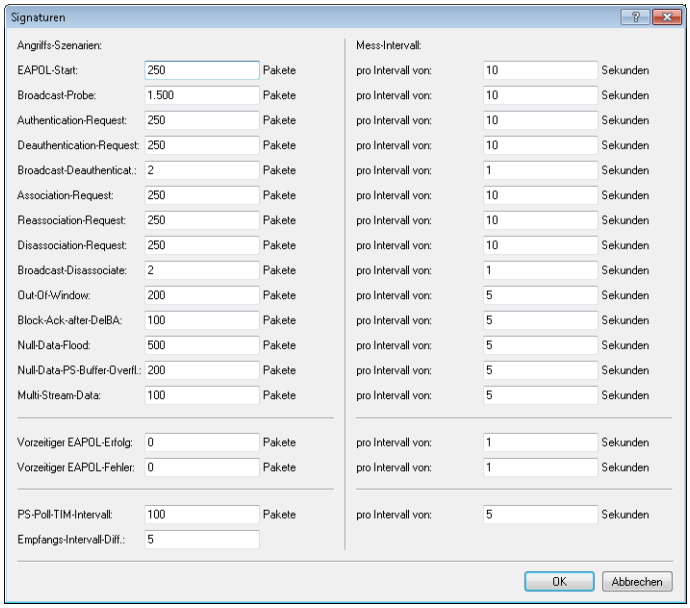
E-Mail-Aggregat-Intervall

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.



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.

3 Ergänzungen im Menüsystem

3.1 Ergänzungen im Setup-Menü

3.1.1 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**

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.

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**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

10

AuthenticateReqFlood

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

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

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

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

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

3.1.2 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-fähige Geräte 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

3.1.3 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**

Ifc

Zeigt das Interface, 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 sollen.

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.

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 Ergänzungen im Status-Menü

3.2.1 Powersave-Wiederholungen

Für jedes aufgrund eines einschränkenden Airtime-Fairness-Modus zurückgestellte Datenpaket erhöht sich der Zähler in dieser Spalte.

SNMP-ID:

1.3.54.29

Pfad Telnet:

Status > **WLAN** > **Fehler**

3.2.2 Adaptive-RF-Optimization

Dieses Menü zeigt bei aktivierter Funktion die Statuswerte der Adaptive-RF-Optimization an.

SNMP-ID:

1.3.126

Pfad Telnet:

Status > **WLAN**

3.2.3 Wireless-IDS

In diesem Verzeichnis finden Sie Statistiken des Wireless Intrusion Detection Systems (WIDS).

SNMP-ID:

1.3.248

Pfad Telnet:

Setup > **WLAN**

Event-Table

Die Event-Tabelle zeigt Ihnen Einzelheiten der letzen Angriffe an, z. B. Ereignistyp, ID und Zeitpunkt des Ereignisses. Ein AP speichert bis zu 100 Einträge.

SNMP-ID:

1.3.248.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Event-Type

Dieser Eintrag zeigt an, um welche Angriffsart es sich gehandelt hat.

SNMP-ID:

1.3.248.1.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Event-Table**

ID

Ereignis-Index mit fortlaufender Nummer für Ereigniseinträge.

SNMP-ID:

1.3.248.1.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Event-Table**

Event-Time

Dieser Eintrag zeigt den Zeitpunkt an, zu dem der Angriff erfolgte.

SNMP-ID:

1.3.248.1.3

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Event-Table**

Event-Rate

Dieser Eintrag zeigt die Anzahl erkannter Angriffe eines Typs während des konfigurierten Zeitraumes an.

SNMP-ID:

1.3.248.1.4

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Event-Table**

Interface

Dieser Eintrag zeigt die Schnittstelle an, über die der Angriff erfolgte.

SNMP-ID:

1.3.248.1.5

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Event-Table**

Signaturen

Dieses Verzeichnis beinhaltet Statistiken über die erkannten Angriffe.

SNMP-ID:

1.3.248.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

AssociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Association-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Association-Request-Angriffe an.

SNMP-ID:

1.3.248.2.1.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.1.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.1.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

ReassociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Reassociation-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

10

Counter

Zeigt die Anzahl der Reassociation-Request-Angriffe an.

SNMP-ID:

1.3.248.2.2.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.2.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.2.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

AuthenticateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Authentication-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Authentication-Request-Angriffe an.

SNMP-ID:

1.3.248.2.3.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.3.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.3.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

EAPOLStart

Dieses Verzeichnis beinhaltet die Statistik über EAPOL-Start-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.4

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der EAPOL-Start-Angriffe an.

SNMP-ID:

1.3.248.2.4.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.4.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.4.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

ProbeBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Probe-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.5

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Probe-Angriffe an.

SNMP-ID:

1.3.248.2.5.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.5.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.5.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

DisassociateBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Disassociate-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.6

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Disassociate-Angriffe an.

SNMP-ID:

1.3.248.2.6.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.6.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.6.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

DeauthenticateBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Deauthenticate-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.7

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Deauthenticate-Angriffe an.

SNMP-ID:

1.3.248.2.7.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.7.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.7.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

DisassociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Disassociation-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.8

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Disassociation-Request-Angriffe an.

SNMP-ID:

1.3.248.2.8.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.8.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.8.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

BlockAckOutOfWindow

Dieses Verzeichnis beinhaltet die Statistik über Out-Of-Window-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.9

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Out-Of-Window-Angriffe an.

SNMP-ID:

1.3.248.2.9.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.9.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.9.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

BlockAckAfterDelBA

Dieses Verzeichnis beinhaltet die Statistik über Block-Ack-after-DelBA-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.10

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Block-Ack-after-DelBA-Angriffe an.

SNMP-ID:

1.3.248.2.10.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.10.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.10.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

NullDataFlood

Dieses Verzeichnis beinhaltet die Statistik über Null-Data-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.11

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Null-Data-Angriffe an.

SNMP-ID:

1.3.248.2.11.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.11.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.11.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

NullDataPSBufferOverflow

Dieses Verzeichnis beinhaltet die Statistik über Null-Data-PS-Buffer-Overflow-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.12

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Null-Data-PS-Buffer-Overflow-Angriffe an.

SNMP-ID:

1.3.248.2.12.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.12.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.12.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

PSPollTIMInterval

Dieses Verzeichnis beinhaltet die Statistik über PS-Poll-TIM-Intervall-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.13

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der PS-Poll-TIM-Intervall-Angriffe an.

SNMP-ID:

1.3.248.2.13.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.13.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.13.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

SMPSMUltiStream

Dieses Verzeichnis beinhaltet die Statistik über Multi-Stream-Data-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.20.14

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Multi-Stream-Data-Angriffe an.

SNMP-ID:

1.3.248.2.14.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.14.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.14.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

DeauthenticateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Deauthentication-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.15

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Deauthentication-Request-Angriffe an.

SNMP-ID:

1.3.248.2.15.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.15.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.15.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

PrematureEAPOLSuccess

Dieses Verzeichnis beinhaltet die Statistik über Vorzeitiger-EAPOL-Erfolg-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.16

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Vorzeitiger-EAPOL-Erfolg-Angriffe an.

SNMP-ID:

1.3.248.2.16.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.16.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.16.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

PrematureEAPOLFailure

Dieses Verzeichnis beinhaltet die Statistik über Vorzeitiger-EAPOL-Fehler-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.17

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Vorzeitiger-EAPOL-Fehler-Angriffe an.

SNMP-ID:

1.3.248.2.17.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.17.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.17.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**