connecting your business

Addendum

LCOS 9.18

LANCOM Systems

Contents

1 Addendum to LCOS version 9.18

This document describes the changes and enhancements in LCOS version 9.18 since the previous version.

For changes in the LCOS menu tree please see section *Enhancements in the menu system* in this Addendum.

2 WLAN

2.1 Adaptive RF Optimization

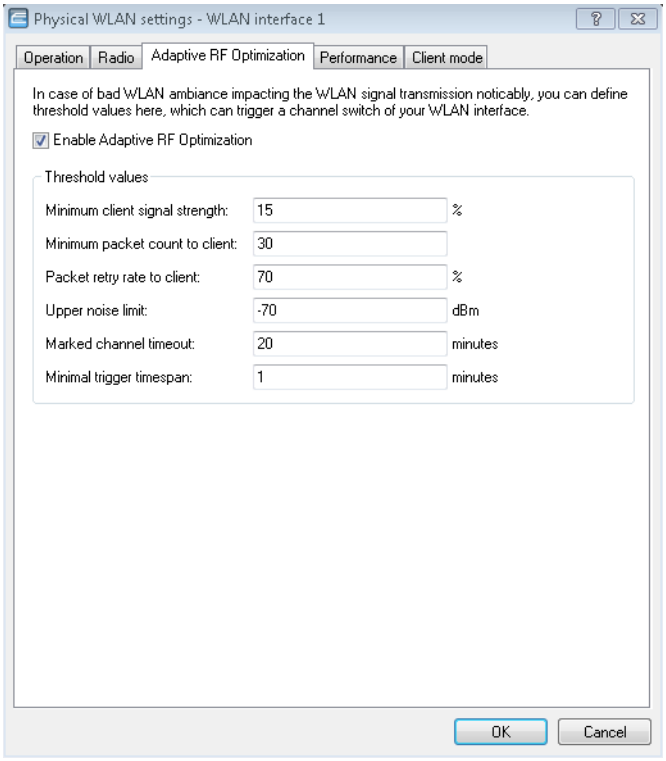
Improved WLAN throughput in the radio field due to dynamic selection of the best WLAN channel by the access point in case of interferences.

By choosing a WLAN channel, the part of the frequency band an access point uses for its logical WLANs is defined. In order to flawlessly operate a WLAN in reach of another access point, each access point should be using a separate channel – otherwise the WLANs have to share the bandwidth of the channel (shared medium). For this purpose, LANCOM access points use the feature Adaptive RF Optimization: The access point permanently scans the radio field for interfering signals. If a certain threshold has been exceeded in the currently used WLAN channel, the access point automatically changes to a qualitatively better channel. This intelligent functionality enables the access point to dynamically adapt to an ever-changing radio field in order to maximize the WLAN's robustness.

In LANconfig you have the option to manually configure the different thresholds on which an automatic channel change is based upon.

2.1.1 Setting up Adaptive RF Optimization with LANconfig

To configure Adaptive RF Optimization open LANconfig and go to **Wireless LAN** > **General**. Click on **Physical WLAN settings** in the section "Interfaces" and select the WLAN interface which you want to configure and go to the tab **Adaptive RF Optimization**.



Enable Adaptive RF Optimization

To enable monitoring of the WLAN radio field via Adaptive RF Optimization, check the box **Enable Adaptive RF Optimization**.

Now you can configure the thresholds which trigger an automatic channel change.

Minimum client signal strength

Setting for the minimal signal strength of clients. When clients with a lower signal strength show up, these will not be considered at the next evaluation and cannot trigger a channel change. The value is set in % with a default of 15.

Minimum packet count to client

Setting for the minimum number of packets sent to a client. If less packets were sent to a client, it will not be considered at the next evaluation and cannot trigger a channel change. The default is 30.

Packet retry rate to client

Setting for the upper limit of resent packets to a client. If a higher percentage of packets had to be resent to clients, the clients' data will be considered at the next evaluation and may trigger a channel change. The value is set in % with a default of 70.

Upper noise limit

Setting for the upper limit of acceptable noise in the channel. The value is set in dBm with a default of -70.

Marked channel timeout

If a channel is considered unusable, it will be marked/blocked for the set amount of time. This value also blocks the channel change trigger in case all channels have been blocked. The value is set in minutes with a default of 20.

Minimal trigger timespan

Setting of the amount of time a limit has to be passed continuously before an action is triggered. In case that no limit was passed during a period of 20 seconds the counted time is being reset. If a limit has been passed for the whole time span the current channel will be blocked/marked. The value is set minutes and with a default of 1.

For this setting we recommend small single digit values.

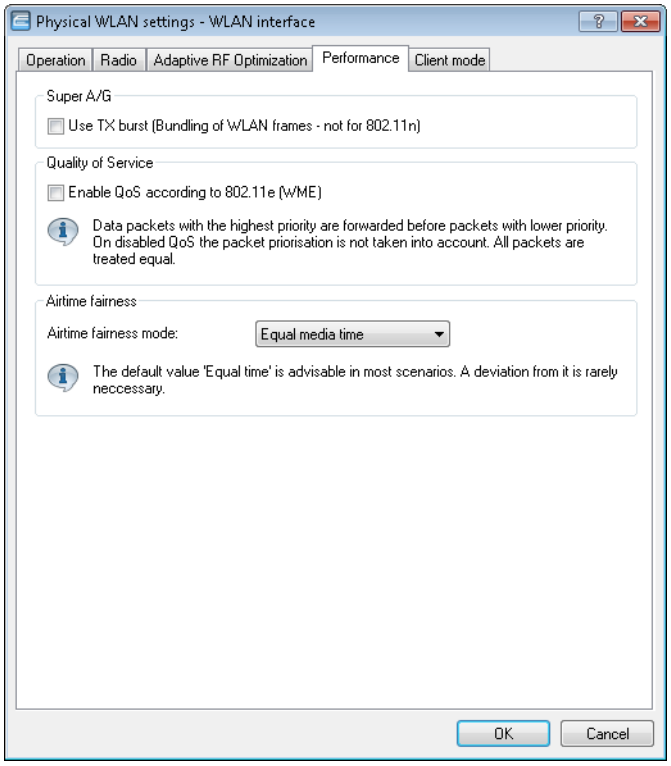
2.2 Airtime Fairness

Efficient usage of the supplied bandwidth due to a fair distribution of the available WLAN transmission times between all active clients, resulting in an increased WLAN performance.

Especially in WLAN scenarios with a high client-density, the devices compete for the available bandwidth. Thereby the sending opportunities are passed around the active clients – without considering necessary transmission times. This leads to slower (legacy) clients slowing down faster clients during the transmission of data packets, although the faster ones could quickly finish their data transmission. The feature Airtime Fairness ensures that the available bandwidth is efficiently used. For that purpose, WLAN transmission times ("airtimes") are fairly distributed among the active clients. The consequence: Thanks to all clients being provided with the same airtime, faster clients can achieve more data throughput in the same amount of time accordingly.

2.2.1 Setting up Airtime Fairness with LANconfig

To configure Airtime Fairness open LANconfig and go to **Wireless LAN** > **General**. Click on **Physical WLAN settings** in the section "Interfaces" and select the WLAN interface which you want to configure and go to the tab **Performance**.



In the section "Airtime fairness" you can select the mode in which Airtime Fairness will operate:

Round robin scheduling

Each client will receive a time slot for transmission one after another.

Equal media time

All clients will receive the same airtime. Clients with a higher data throughput will benefit from this setting because the access point can send more data to the client in the same time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

802.11n preferred

This setting prefers clients using IEEE 802.11n. Clients that just use IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b will only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

Equal media volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down all clients.

This setting is only recommended when it is necessary that all clients receive the same throughput.

2.3 Wireless Intrusion Detection System (WIDS)

An Intrusion Detection System (IDS) recognizes attacks on a network and reports these attacks to a network management system. Especially in a professional environment an IDS is mandatory to be able to detect and deal with possible attacks or interferences directly.

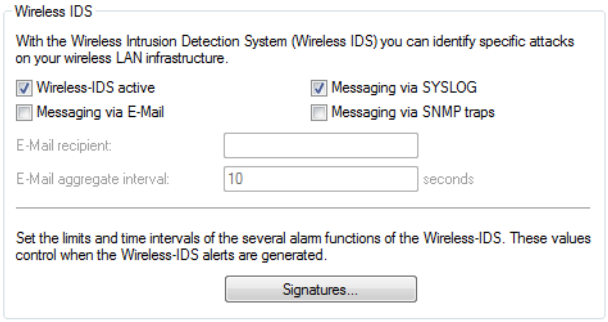
The Wireless Intrusion Detection System (WIDS) in LANCOM devices monitors the different WLANs by using a wide range of different thresholds. If a possible attack is detected, it will be reported directly via e-mail, SYSLOG, or SNMP traps.

The detection of attacks is based on known and similar patterns.

Please take notice that detection based on pattern recognition (heuristics) can lead to false alarms (false positives)!

2.3.1 Setting up the Wireless Intrusion Detection System with LANconfig

To configure the Wireless Intrusion Detection System (WIDS) open LANconfig and go to **Wireless LAN** > **Security**. In the section "Wireless IDS" you will find the configuration options.



Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG. The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

Messaging via SNMP traps

Activates or deactivates the messaging via SNMP traps. The generated message contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

Messaging via E-Mail

Activates or deactivates the messaging via e-mail. The generated e-mail contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

An SMTP account has to be configured to be able to use messaging via e-mail.

E-Mail recipient

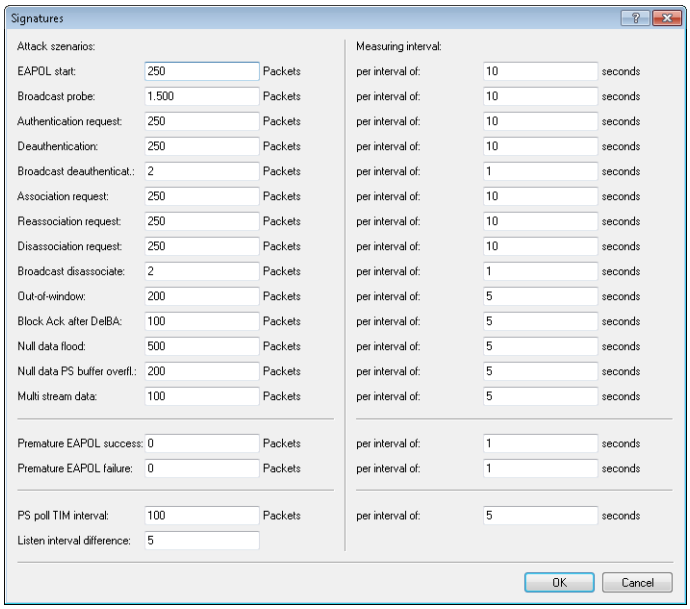
The e-mail address of the recipient when messaging via e-mail is activated.

E-Mail aggregate interval

This setting sets the delay before a new e-mail is sent in case the WIDS is triggered again. This prevents flooding by e-mail in case of extensive attacks.

Signatures

Here you can configure the various thresholds and measuring intervals (packets per second) of the different alarm functions of the WIDS. These settings are used by the WIDS to determine if an attack is taking place.



The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

- EAPOL-Start
- Broadcast probe
- Authentication request
- Deauthentication
- Broadcast deauthentication
- 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
- Premature EAPOL success
- Premature EAPOL failure
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.

3 Enhancements in the menu system

3.1 Additions to the Setup menu

3.1.1 Wireless-IDS

In this directory, you configure the Wireless Intrusion Detection System (WIDS).

SNMP ID:

2.12.248

Telnet path:

Setup > **WLAN**

IDS-Operational

Activates or deactivates the Wireless Intrusion Detection System (WIDS).

SNMP ID:

2.12.248.9

Telnet path:

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

Possible values:

No

The Wireless Intrusion Detection System is deactivated.

Yes

The Wireless Intrusion Detection System is activated.

Default:

No

Syslog-Operational

Activates or deactivates the messaging via SYSLOG. The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

SNMP ID:

2.12.248.10

Telnet path:

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

Possible values:

No

Messaging via SYSLOG is disabled.

Yes

Messaging via SYSLOG is enabled.

Default:

Yes

SNMPTraps-Operational

Activates or deactivates the messaging via SNMP traps. The generated message contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

SNMP ID:

2.12.248.11

Telnet path:

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

Possible values:

No

Messaging via SNMP traps is disabled.

Yes

Messaging via SNMP traps is enabled.

Default:

No

E-Mail

Activates or deactivates the messaging via E-Mail. The generated E-Mail contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

An SMTP account has to be configured to be able to use messaging via E-Mail.

SNMP ID:

2.12.248.12

Telnet path:

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

Possible values:

No

Messaging via e-mail is disabled.

Yes

Messaging via e-mail is enabled.

Default:

No

E-Mail-Receiver

The E-Mail address of the recipient when messaging via E-Mail is activated.

SNMP ID:

2.12.248.13

Telnet path:

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

Possible values:

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

E-Mail-Aggregate-Interval

This setting sets the delay in seconds before a new E-Mail is sent in case the WIDS is triggered again. This prevents flooding by E-Mail in case of extensive attacks.

SNMP ID:

2.12.248.14

Telnet path:

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

Possible values:

max. 4 characters from `[0-9]`

Default:

10

Signatures

Here you can configure the various thresholds and measuring intervals (packets per second) of the different alarm functions of the WIDS. These settings are used by the WIDS to determine if an attack is taking place.

SNMP ID:

2.12.248.50

Telnet path:

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

AssociateReqFlood

Here you can configure the threshold for attacks of the type **AssociateReqFlood**.

SNMP ID:

2.12.248.50.1

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.1.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.1.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

ReassociateReqFlood

Here you can configure the threshold for attacks of the type **ReassociateReqFlood**.

SNMP ID:

2.12.248.50.2

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.2.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.2.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

AuthenticateReqFlood

Here you can configure the threshold for attacks of the type **AuthenticateReqFlood**.

SNMP ID:

2.12.248.50.3

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.3.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.3.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

EAPOLStart

Here you can configure the threshold for attacks of the type **EAPOLStart**.

SNMP ID:

2.12.248.50.4

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.4.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.4.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

ProbeBroadcast

Here you can configure the threshold for attacks of the type **ProbeBroadcast**.

SNMP ID:

2.12.248.50.5

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.5.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

1500

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.5.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

DisassociateBroadcast

Here you can configure the threshold for attacks of the type **DisassociateBroadcast**.

SNMP ID:

2.12.248.50.6

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.6.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

2

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.6.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

1

DeauthenticateBroadcast

Here you can configure the threshold for attacks of the type **DeauthenticateBroadcast**.

SNMP ID:

2.12.248.50.7

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.7.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

2

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.7.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

Possible values:

max. 4 characters from `[0-9]`

Default:

1

DisassociateReqFlood

Here you can configure the threshold for attacks of the type **DisassociateReqFlood**.

SNMP ID:

2.12.248.50.8

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.8.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.8.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

BlockAckOutOfWindow

Here you can configure the threshold for attacks of the type **BlockAckOutOfWindow**.

SNMP ID:

2.12.248.50.9

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.9.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

Possible values:

max. 4 characters from `[0-9]`

Default:

200

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.9.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

BlockAckAfterDelBA

Here you can configure the threshold for attacks of the type **BlockAckAfterDelBA**.

SNMP ID:

2.12.248.50.10

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.10.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

Possible values:

max. 4 characters from `[0-9]`

Default:

100

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.10.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

NullDataFlood

Here you can configure the threshold for attacks of the type **NullDataFlood**.

SNMP ID:

2.12.248.50.11

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.11.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

500

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.11.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

NullDataPSBufferOverflow

Here you can configure the threshold for attacks of the type **NullDataPSBufferOverflow**.

SNMP ID:

2.12.248.50.12

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.12.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

Possible values:

max. 4 characters from `[0-9]`

Default:

200

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.12.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

PSPollTIMInterval

Here you can configure the threshold for attacks of the type **PSPollTIMInterval**.

SNMP ID:

2.12.248.50.13

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.13.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

max. 4 characters from `[0-9]`

Default:

100

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.13.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

Intervall-Diff

SNMP ID:

2.12.248.50.13.3

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

SMPSMUltiStream

Here you can configure the threshold for attacks of the type **SMPSMUltiStream**.

SNMP ID:

2.12.248.50.14

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.14.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMUltiStream**

Possible values:

max. 4 characters from `[0-9]`

Default:

100

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.14.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMUltiStream**

Possible values:

max. 4 characters from `[0-9]`

Default:

5

DeauthenticateReqFlood

Here you can configure the threshold for attacks of the type **DeauthenticateReqFlood**.

SNMP ID:

2.12.248.50.15

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.15.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

250

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.15.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

PrematureEAPOLSuccess

Here you can configure the threshold for attacks of the type **PrematureEAPOLSuccess**.

SNMP ID:

2.12.248.50.16

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.16.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLSuccess**

Possible values:

max. 4 characters from `[0-9]`

Default:

2

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.16.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLSuccess**

Possible values:

max. 4 characters from `[0-9]`

Default:

1

PrematureEAPOLFailure

Here you can configure the threshold for attacks of the type **PrematureEAPOLFailure**.

SNMP ID:

2.12.248.50.17

Telnet path:

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

CounterLimit

Set the threshold of packets, at which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.17.1

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLFailure**

Possible values:

max. 4 characters from `[0-9]`

Default:

2

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.17.2

Telnet path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLFailure**

Possible values:

max. 4 characters from `[0-9]`

Default:

1

Promiscuous-Mode

Activates or deactivates the promiscuous mode. When it is enabled, even packets not send to the access point will be forwarded to LCOS for analysis by the WIDS.

This mode can be used to detect the following attacks:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess

Please note, the promiscuous mode will have a large impact on the performance. For example, frame aggregation will be deactived when using it. Therefore, use this mode only in case of a strong suspicion.

SNMP ID:

2.12.248.51

Telnet path:

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

Possible values:

No

The Promiscuous-Mode is deactivated.

Yes

The Promiscuous-Mode is activated.

Default:

No

3.1.2 Airtime-Fairness-Modus

Efficient usage of the supplied bandwidth due to a fair sharing of the available WLAN transmission times between all active clients results in an increased WLAN performance. **Airtime Fairness** is activated by default.

SNMP ID:

2.23.20.9.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Performance**

Possible values:

Round-Robin

Each client will receive one after another a time slot for transmission.

Equal-Airtime

All clients will receive the same airtime. Clients with a higher data throughput will profit from this setting because the access point can send more data to the client in the same time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

Pref.-11n-Airtime

This setting prefers clients using IEEE 802.11n. Clients that just use IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b will only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

Equal-Volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down all clients.

This setting is only recommended when it is necessary that all clients receive the same throughput.

Default:

Equal-Airtime

3.1.3 Adaptive-RF-Optimization

Adaptive RF Optimizationmonitors the WLAN environment on a constant basis and evaluates the quality of the network based on the "Wireless Quality Indicators". If the quality drops, the Adaptive RF Optimization triggers a channel change to improve the quality again.

SNMP ID:

2.23.20.23

Telnet path:

Setup > **Interfaces** > **WLAN**

Ifc

Shows the interface for the Adaptive RF Optimization.

SNMP ID:

2.23.20.23.1

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Operating

Activates or deactivates Adaptive RF Optimization for this interface.

SNMP ID:

2.23.20.23.2

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

No

Adaptive RF Optimization for this interface is deactivated.

Yes

Adaptive RF Optimization for this interface is activated.

Default:

No

Min-Client-Phy-Signal

Setting for the minimal signal strength of clients.

SNMP ID:

2.23.20.23.3

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 3 characters from `[0-9]`

Default:

15

Min-Client-Tx-Packets

Setting for the minimum number of packets sent to a client.

SNMP ID:

2.23.20.23.4

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 5 characters from `[0-9]`

Default:

30

Tx-Client-Retry-Ratio-Limit

Setting for the upper limit of resent packets to a client.

SNMP ID:

2.23.20.23.5

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 3 characters from `[0-9]`

Default:

70

Noise-Limit

Setting for the upper limit of acceptable noise in the channel.

SNMP ID:

2.23.20.23.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 6 characters from `[0-9] -`

Default:

-70

Marked-Channel-Timeout

When a channel is considered unusable it is marked/blocked for the set amount of time.

SNMP ID:

2.23.20.23.7

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 5 characters from `[0-9]`

Default:

20

Trigger-Timespan

Setting of the amount of time a limit has to be passed continuously before an action is triggered.

SNMP ID:

2.23.20.23.8

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

max. 5 characters from `[0-9]`

Default:

1

3.2 Additions to the Status menu

3.2.1 Powersave-Retransmits

For each packet postponed based on an Airtime Fairness mode the counter will increase by 1.

SNMP ID:

1.3.54.29

Telnet path:

Status > **WLAN** > **Errors**

3.2.2 Adaptive-RF-Optimization

This menu shows the status entries of the Adaptive RF Optimization when it is activated.

SNMP ID:

1.3.126

Telnet path:

Status > **WLAN**

3.2.3 Wireless-IDS

In this directory, you find the statistics of the Wireless Intrusion Detection System (WIDS).

SNMP ID:

1.3.248

Telnet path:

Status > **WLAN**

Event-Table

The event table shows the details of the last 100 attacks. This includes event type, event ID, and timestamp of the event.

SNMP ID:

1.3.248.1

Telnet path:

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

Event-Type

This entry shows the type of attack.

SNMP ID:

1.3.248.1.1

Telnet path:

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

ID

Index to identify the events.

SNMP ID:

1.3.248.1.2

Telnet path:

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

Event-Time

Time when the attack took place.

SNMP ID:

1.3.248.1.3

Telnet path:

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

Event-Rate

This entry shows the rate of the attack during the configured interval.

SNMP ID:

1.3.248.1.4

Telnet path:

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

Interface

This entry shows the interface on which the attack took place.

SNMP ID:

1.3.248.1.5

Telnet path:

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

Signatures

This directory holds information about the different attacks.

SNMP ID:

1.3.248.2

Telnet path:

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

AssociateReqFlood

In this directory, you find the statistics of the attack of the type **AssociateReqFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.1

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.1.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.1.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.1.3

Telnet path:

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

ReassociateReqFlood

In this directory, you find the statistics of the attack of the type **ReassociateReqFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.2

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Possible values:

max. 4 characters from `[0-9]`

Default:

10

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.2.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.2.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.2.3

Telnet path:

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

AuthenticateReqFlood

In this directory, you find the statistics of the attack of the type **AuthenticateReqFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.3

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.3.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.3.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.3.3

Telnet path:

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

EAPOLStart

In this directory, you find the statistics of the attack of the type **EAPOLStart**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.4

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.4.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.4.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.4.3

Telnet path:

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

ProbeBroadcast

In this directory, you find the statistics of the attack of the type **ProbeBroadcast**.

SNMP ID:

1.3.248.2.5

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.5.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.5.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.5.3

Telnet path:

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

DisassociateBroadcast

In this directory, you find the statistics of the attack of the type **DisassociateBroadcast**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.6

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.6.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.6.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.6.3

Telnet path:

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

DeauthenticateBroadcast

In this directory, you find the statistics of the attack of the type **DeauthenticateBroadcast**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.7

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.7.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.7.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.7.3

Telnet path:

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

DisassociateReqFlood

In this directory, you find the statistics of the attack of the type **DisassociateReqFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.8

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.8.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.8.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.8.3

Telnet path:

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

BlockAckOutOfWindow

In this directory, you find the statistics of the attack of the type **BlockAckOutOfWindow**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.9

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.9.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.9.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.9.3

Telnet path:

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

BlockAckAfterDelBA

In this directory, you find the statistics of the attack of the type **BlockAckAfterDelBA**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.10

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.10.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.10.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.10.3

Telnet path:

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

NullDataFlood

In this directory, you find the statistics of the attack of the type **NullDataFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.11

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.11.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.11.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.11.3

Telnet path:

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

NullDataPSBufferOverflow

In this directory, you find the statistics of the attack of the type **NullDataPSBufferOverflow**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.12

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.12.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.12.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.12.3

Telnet path:

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

PSPollTIMInterval

In this directory, you find the statistics of the attack of the type **PSPollTIMInterval.**

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.13

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.13.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.13.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.13.3

Telnet path:

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

SMPSMUltiStream

In this directory, you find the statistics of the attack of the type **SMPSMUltiStream**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.20.14

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.14.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.14.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.14.3

Telnet path:

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

DeauthenticateReqFlood

In this directory, you find the statistics of the attack of the type **DeauthenticateReqFlood**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.15

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.15.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.15.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.15.3

Telnet path:

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

PrematureEAPOLSuccess

In this directory, you find the statistics of the attack of the type **PrematureEAPOLSuccess**.

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.16

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.16.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.16.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.16.3

Telnet path:

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

PrematureEAPOLFailure

In this directory, you find the statistics of the attack of the type **PrematureEAPOLFailure.**

The display of the parameters may vary depending on the number of interfaces.

SNMP ID:

1.3.248.2.17

Telnet path:

Status > **WLAN** > **Wireless-IDS** > **Signatures**

Counter

Number of recorded attacks.

SNMP ID:

1.3.248.2.17.1

Telnet path:

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

Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

SNMP ID:

1.3.248.2.17.2

Telnet path:

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

Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

SNMP ID:

1.3.248.2.17.3

Telnet path:

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