



**HIRSCHMANN**

A **BELDEN** BRAND

# White Paper

## Rogue AP and Rogue Client Detection WLAN Access Point

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2010 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site ([www.hirschmann-ac.de](http://www.hirschmann-ac.de)).

Printed in Germany  
Hirschmann Automation and Control GmbH  
Stuttgarter Str. 45-51  
72654 Neckartenzlingen  
Germany  
Tel.: +49 1805 141538

# **Rogue AP and Rogue Client Detection**

Now widespread, the use of WLAN technology is leading to a high density of neighboring wireless networks. WLAN signals can come from a variety of unknown sources—from neighboring companies, from a visitor with a notebook equipped with WLAN, or even from somebody attacking your company network.

Rogue access points and rogue clients can seriously interfere with company networks, and even cause considerable damage to the company's well-being. Poorly configured WLAN components can provide an unintended method of access to the company network for intruders or competitors.

Administrators of WLAN structures need a mechanism which helps to quickly and reliably identify rogue access points and rogue clients.

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues.

- ▶ Rogue clients are computers equipped with WLAN adapters that are located within the range of a WLAN and attempt to log on to one of the access points, for example, in order to use the Internet connection or in order to receive access to secured areas on the network.
- ▶ An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but at least disturbing are access points that belong to third-party networks within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

The screenshot shows the WLANmonitor application window. On the left, a tree view under 'Groups' shows 'Rogue AP Detection' expanded, with sub-items like 'All APs (111)', 'New APs', 'Rogue APs', 'Unknown APs', 'Known APs', and 'Own APs'. The main pane displays a table of detected Rogue APs. The table has columns: Last Seen, Identification, Network Name (S...), Band, Cha..., Encry..., 108..., and First Seen. A tooltip is visible over one of the rows, showing details for the IP address 10.1.10.188, including the interface (WLAN-1) and signal strength (18 %).

Last Seen	Identification	Network Name (S...)	Band	Cha...	Encry...	108...	First Seen
18.08.2006 15:45:49	Client01	Network01	2,4 GHz	11	None	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client02	Network01	2,4 GHz	11	None	No	29.06.2006 11:46:02
03.07.2006 16:39:05	Client03	Network01	5 GHz	100	AES	No	03.07.2006 15:29:43
03.07.2006 16:39:05	Client04	Network01	5 GHz	100	AES	No	03.07.2006 15:29:43
04.07.2006 18:16:46	Client01	Network02	2,4 GHz	11	None	No	03.07.2006 15:29:47
09.08.2006 15:39:52	Client02	Network02	2,4 GHz	11	None	No	09.08.2006 14:49:27
18.08.2006 15:45:44	Client03	10.1.1.31: Interface: WLAN-1, Signal: 50 %	2,4 GHz	11	AES+TKIP	No	10.08.2006 18:58:49
11.08.2006 09:15:06	Client04	10.1.10.193: Interface: WLAN-1, Signal: 10 %	2,4 GHz	11	None	No	10.08.2006 18:58:50
11.08.2006 12:27:58	Client01	10.1.10.192: Interface: WLAN-1, Signal: 31 %	2,4 GHz	11	None	No	11.08.2006 10:06:49
18.08.2006 15:46:03	Client02	10.1.10.189: Interface: WLAN-1, Signal: 45 %	2,4 GHz	11	None	No	18.08.2006 12:40:46
18.08.2006 15:46:03	Client03	10.1.10.188: Interface: WLAN-1, Signal: 18 %	2,4 GHz	11	None	No	18.08.2006 12:40:46
18.08.2006 15:45:20	Client04	2,4 GHz 11	2,4 GHz	11	None	No	18.08.2006 12:40:50
18.08.2006 15:45:20	Client01	Network04	2,4 GHz	11	None	No	18.08.2006 14:54:08
18.08.2006 15:45:44	Client02	Network04	2,4 GHz	5	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client03	Network04	2,4 GHz	7	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client04	Network04	2,4 GHz	7	WEP	No	29.06.2006 11:46:02
11.08.2006 12:28:44	Client01	2,4 GHz 11	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client02	2,4 GHz 3	2,4 GHz	3	WEP	No	03.07.2006 15:29:44
13.07.2006 09:11:34	Client03	2,4 GHz 1	2,4 GHz	1	WEP	No	12.07.2006 23:10:24
18.08.2006 15:45:44	Client04	2,4 GHz 11	2,4 GHz	11	WEP	No	18.08.2006 15:44:35
15.07.2006 11:33:43	Client01	2,4 GHz 6	2,4 GHz	6	WEP	No	29.06.2006 11:46:02
04.07.2006 18:16:53	Client02	2,4 GHz 11	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
04.07.2006 18:16:53	Client03	2,4 GHz 11	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
15.07.2006 11:33:43	Client04	2,4 GHz 11	2,4 GHz	11	AES	No	12.07.2006 23:10:21
11.08.2006 09:15:06	Client01	5 GHz 140	5 GHz	140	AES+TKIP	No	09.08.2006 14:49:19
18.08.2006 15:45:44	Client02	2,4 GHz 6	2,4 GHz	6	WEP	No	09.08.2006 14:49:21
18.08.2006 15:45:44	Client03	2,4 GHz 11	2,4 GHz	11	WEP	No	18.08.2006 12:40:34
18.08.2006 15:45:49	Client04	5 GHz 100	5 GHz	100	AES	No	29.06.2006 11:45:56
18.08.2006 15:45:44	Client01	2,4 GHz 1	2,4 GHz	1	AES+TKIP	No	29.06.2006 11:46:02
18.08.2006 15:45:44	Client02	2,4 GHz 1	2,4 GHz	1	AES	No	29.06.2006 11:46:02
18.08.2006 15:45:44	Client03	2,4 GHz 1	2,4 GHz	1	AES	No	29.06.2006 11:46:02

Figure 1: Screenshot WLANmonitor

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least they are a disturbance, and so they need to be identified to decide whether further measures in securing the local network need to be introduced. Information about the clients within range of your network is automatically stored to an internal table in the WLAN device. Once activated, background scanning records neighboring access points and records them to the scan table. WLANmonitor presents this information visually. The access points and clients found can be categorized in groups such as 'known', 'unknown' or 'rogue'.

## ■ Rogue AP Detection

WLANmonitor sorts all of the access points found into predefined subgroups under 'Rogue AP Detection' while displaying the following information:

- ▶ Time of first and last detection
- ▶ BSSID, the MAC address of the AP for this WLAN network

- ▶ Network name
- ▶ Type of encryption used
- ▶ Frequency band used
- ▶ Radio channel used
- ▶ Use of 108 Mbps mode

**Note:** To use rogue AP detection, background scanning has to be activated in the WLAN device.

The WLANmonitor uses the following groups for sorting the APs that are found:

- ▶ All APs: List of all scanned WLAN networks grouped as follows
- ▶ New APs: New unknown and unconfigured WLAN networks are automatically grouped here (APs displayed in yellow)
- ▶ Rogue APs: WLAN networks identified as rogue and in need of urgent observation (APs displayed in red)
- ▶ Unknown APs: WLAN networks which are to be further analyzed (APs displayed in gray)
- ▶ Known APs: WLAN networks which are not a threat (APs displayed in gray)
- ▶ Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (APs displayed in green)

The WLANs that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All APs').

**Note:** If a parameter is being changed for an access point (e.g. security settings) this access point will be displayed in the list on new APs.

### ■ **Rogue client detection**

Der WLANmonitor presents all of the clients found into predefined subgroups under 'Rogue Client Detection' while displaying the following information:

- ▶ Time of first and last detection
- ▶ MAC address of the client
- ▶ Network name

**Note:** No configuration of the WLAN device is necessary to make use of rogue client detection.

The WLANmonitor uses the following groups for sorting the clients that are found:

- ▶ All clients: List of all found clients grouped as follows (clients are colored according to their group)
- ▶ New clients: New unknown clients are automatically grouped here (clients displayed in yellow)
- ▶ Rogue clients: Clients identified as rogue and in need of urgent observation (clients displayed in red)
- ▶ Unknown clients: Clients which are to be further analyzed (clients displayed in gray)
- ▶ Known clients: Clients which are not a threat (clients displayed in gray)
- ▶ Own clients: New affiliated clients associated with access points monitored by WLAN monitor are automatically grouped here (APs displayed in green)

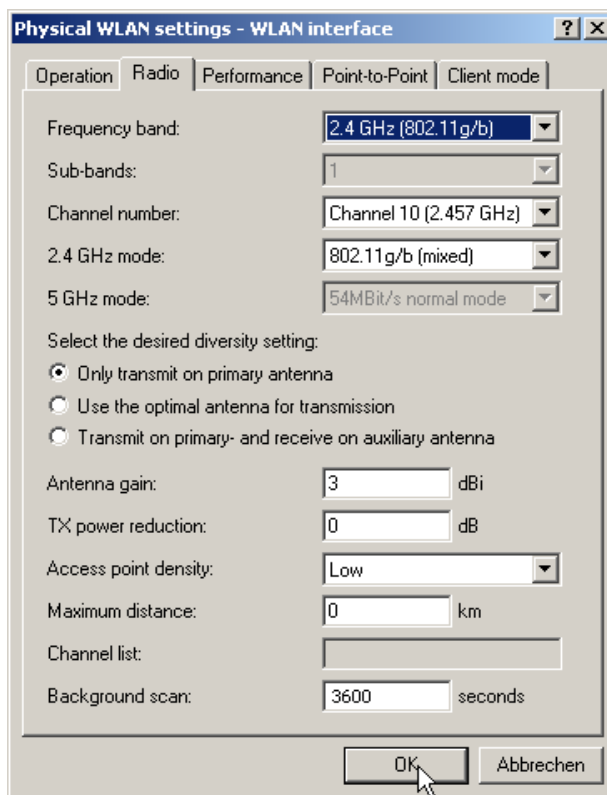
The clients that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All clients').

### ■ **Background WLAN Scanning**

The clients that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All clients').

The information on the access points found can be viewed in the WLANmonitor or in the WLAN device's statistics.

When configuring the background scan, a time period is defined in which all available WLAN channels are to be scanned once for the receiving beacons.



*Figure 2: Physical WLAN settings for background scanning*

To avoid adverse effects on data transfer rates, the interval between channel scans should be at least 20 seconds. Lesser values will be corrected to this minimum value automatically. For example, with 13 channels to scan in the 2.4 GHz band, one scan of the full spectrum takes at least  $13 \times 20 \text{ s} = 260 \text{ seconds}$ . Background scanning can be limited to a lower number of channels when indoor mode is activated.

**Note:** The background scanning can be reduced to a smaller number of channels if the indoor mode is activated or a list of allowed channels is defined.





## A Further support

### ■ Technical questions and training courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.

You can find the addresses of our distributors on the Internet:

[www.hirschmann-ac.com](http://www.hirschmann-ac.com).

Our support line is also at your disposal:

- ▶ Tel. +49 1805 14-1538
- ▶ Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site ([www.hirschmann-ac.com](http://www.hirschmann-ac.com)) at the end of the product sites in the FAQ category.

The current training courses to technology and products can be found under <http://www.hicomcenter.com>.

### ■ Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- ▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- ▶ Training offers you an introduction to the basics, product briefing and user training with certification.
- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>.



**HIRSCHMANN**

---

A **BELDEN** BRAND