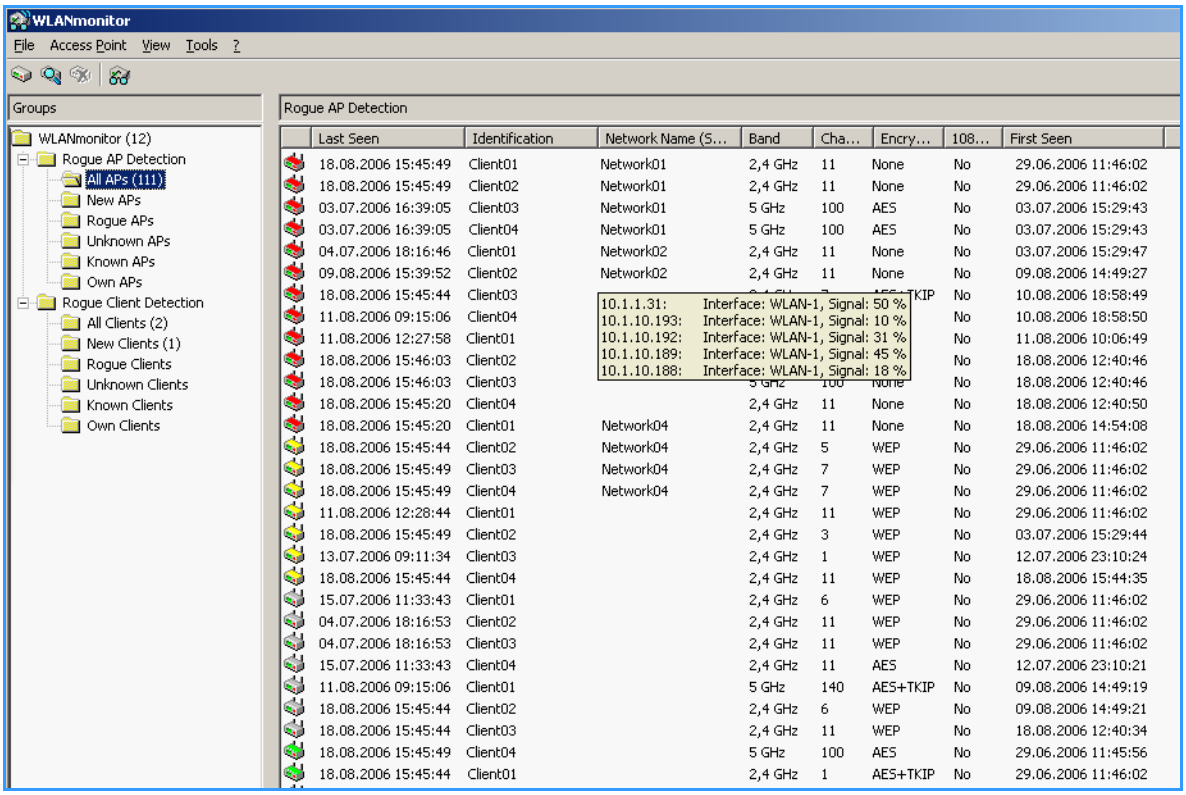
LANCOM™ Techpaper
Rogue AP and Rogue Client Detection

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.

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 LANCOM Wireless Router. 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'.



LANCOM Systems

LANCOM™ Techpaper
Rogue AP and Rogue Client Detection

Rogue AP detection

The 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 addresse of the AP for this WLAN network
- Network name
- Type of encryption used
- Frequency band used
- Radio channel used
- Use of 108 Mbps mode

To use rogue AP detection, background scanning has to be activated in the LANCOM Wireless Router.

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').

Rogue client detection

The 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

No configuration of the LANCOM Wireless Router 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').

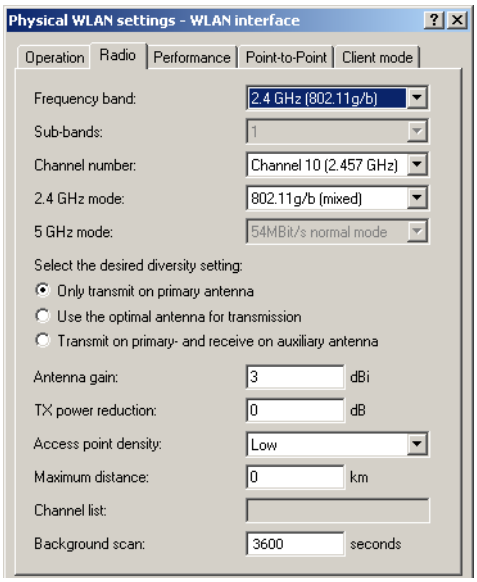
LANCOM™ Techpaper
Rogue AP and Rogue Client Detection

Background WLAN Scanning

In order to identify other access points within the device's local radio range, the LANCOM Wireless Router can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

The information on the access points found can be viewed in the WLANmonitor or in the LANCOM Wireless Router 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.



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 x 20s = 260 seconds.

Background scanning can be limited to a lower number of channels when indoor mode is activated.