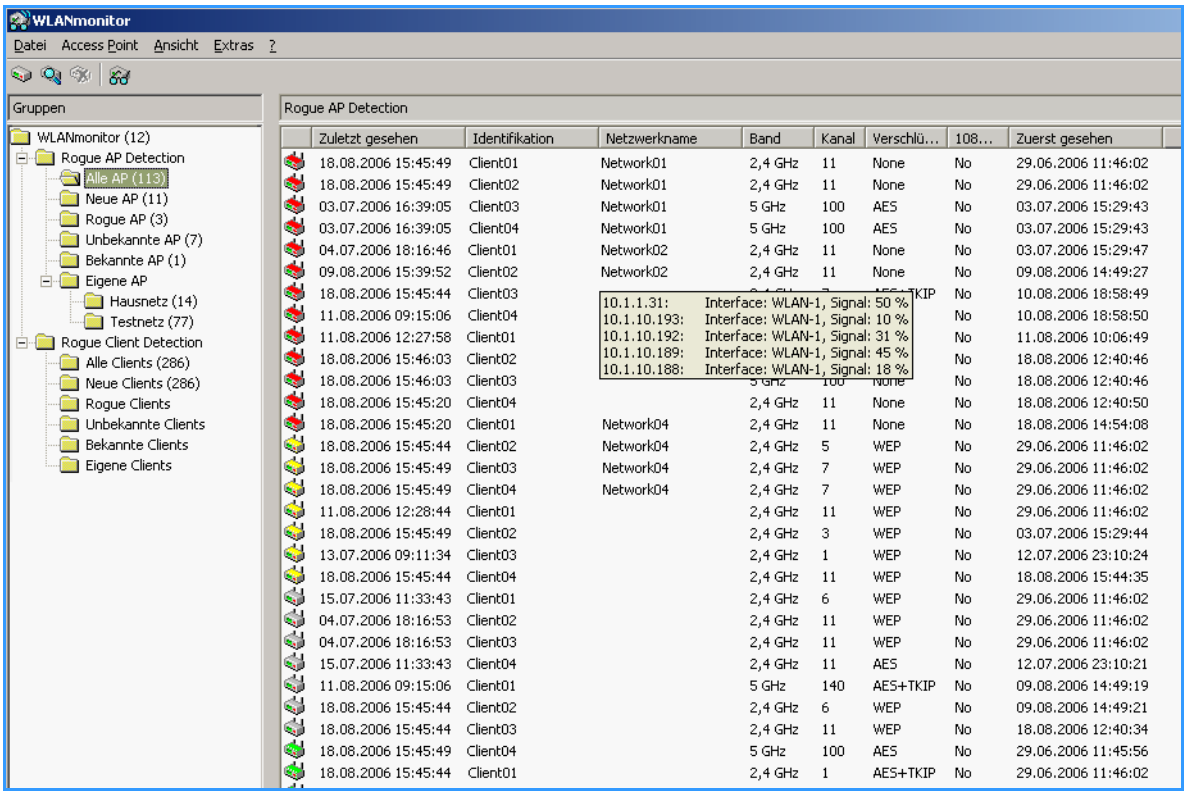
LANCOM™ Techpaper
Rogue AP und Rogue Client Detection

Die inzwischen weit verbereitete Nutzung der WLAN-Technik führt zu einer hohen Dichte der benachbarten Funknetzwerke. WLAN-Signale von unbekannten Teilnehmern können aus ganz unterschiedlichen Quellen stammen – von der benachbarten Firma, von einem Besucher mit WLAN-Schnittstelle im Notebook oder einem Angreifer auf das eigene Unternehmens-Netzwerk.
Rogue Access Points und Rouge Clients können drahtlose Firmen-Netzwerke empfindlich stören und dem Unternehmen ernsthaften Schaden zufügen. Ungenügend konfigurierte Wireless LAN-Komponenten können z.B. unbewußt einen Zugang für Eindringlinge oder Wettbewerber in das Firmennetzwerk öffnen.
Die Administratoren von WLAN-Strukturen benötigen einen Mechanismus, mit dem Rogue Access Points und Rouge Clients schnell und zuverlässig erkannt werden können.

Als 'Rogue' (engl. für Schurke, Gauner) bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als Access Point oder Client Teilnehmer in einem WLAN zu werden.

- Bei Rogue Clients versuchen Rechner mit WLAN-Adapter in der Reichweite des eigenen WLAN, sich bei einem der Access Points einzubuchen, um z.B. die Internetverbindung mit zu nutzen oder Zugang zu geschützten Bereichen des Netzwerks zu erhalten.
- Rogue APs sind solche Access Points, die z.B. von den Mitarbeitern einer Firma ohne Kenntnis und Erlaubnis der System-Administratoren an das Netzwerk angeschlossen werden und so über ungesicherte WLAN-Zugänge bewusst oder unbewusst Tür und Tor für potentielle Angreifer öffnen. Nicht ganz so gefährlich, aber zumindest störend sind z.B. Access Points in der Reichweite des eigenen WLAN, die zu fremden Netzwerken gehören. Verwenden solche Geräte dabei z.B. die gleiche SSID und den gleichen Kanal wie die eigenen APs (Default-Einstellungen), können die eigenen WLAN-Clients versuchen, sich bei dem fremden Netzwerk einzubuchen.

Da alle unbekannten Clients und Access Points in der Reichweite des eigenen Netzwerks eine mögliche Bedrohung und Sicherleitslücke, zumindest aber eine Störung darstellen, müssen diese Geräte erkannt werden, um ggf. weitere Maßnahmen zur Sicherung des eigenen Netzwerks einzuleiten. Die Informationen über die Clients in der Reichweite des eigenen Netzwerks werden automatisch in den internen Tabellen des LANCOM Wireless Router gespeichert. Mit der Aktivierung des Background-Scanning werden auch die benachbarten Access Points erfasst und in der Scan-Tabelle gespeichert. Mit dem WLANmonitor können diese Informationen sehr komfortabel visualisiert werden, die Access Points und Clients können dabei z.B. in Kategorien wie 'bekannt', 'unbekannt' oder 'rogue' eingeteilt werden.



LANCOM Systems

LANCOM™ Techpaper
Rogue AP und Rogue Client Detection

Rogue AP Detection

Der WLANmonitor stellt alle gefundenen Access Points in vordefinierten Untergruppen von 'Rogue AP Detection' dar und zeigt dabei u.a. folgende Informationen:

- Zeitpunkt der ersten und letzten Erkennung
- BSSID, also MAC-Adresse des AP für dieses WLAN-Netz
- Netzwerkname
- verwendete Verschlüsselung
- verwendetes Frequenzband
- verwendeter Funk-Kanal
- Verwendung des 108Mbps-Modus

Für die Nutzung der Rogue AP Detection muss im LANCOM Wireless Router das Background Scanning aktiviert werden (s.u.).

Folgende Gruppen nutzt der WLANmonitor zur Sortierung der gefundenen APs:

- Alle APs: Auflistung aller gescannter WLAN-Netze der folgenden Gruppen
- Neue APs: neue unbekannte und unkonfigurierte WLAN-Netze gelangen automatisch in diese Gruppe (die APs werden gelb dargestellt)
- Rogue APs: WLAN-Netze, die als Rogue erkannt und dringend zu beobachten sind (die APs werden rot dargestellt)
- Unbekannte APs: WLAN-Netze, bei denen weitere Untersuchungen notwendig sind (die APs werden grau dargestellt)
- Bekannte APs: WLAN-Netze, die keine Gefahr darstellen (die APs werden grau dargestellt)
- Eigene APs: neue eigene WLAN-Netze von Access Points, die der WLANmonitor beobachtet, gelangen automatisch in diese Gruppe (die APs werden grün dargestellt)

Die gefundenen WLAN-Netze können je nach Status in eine entsprechende Gruppe verschoben werden. Innerhalb der einzelnen Gruppen können über das Kontextmenü (rechte Maustaste) eigene Gruppen angelegt werden (ausgenommen der Gruppe 'Alle APs').

Wenn sich bei einem AP ein Parameter ändert, z.B. die Sicherheitseinstellung, dann wird er wieder als neu gefundener AP angezeigt.

Rogue Client Detection

Der WLANmonitor stellt alle gefundenen Clients in vordefinierten Untergruppen von 'Rogue Client Detection' dar und zeigt dabei u.a. folgende Informationen:

- Zeitpunkt der ersten und letzten Erkennung
- MAC-Adresse des Clients
- Netzwerkname

Für die Nutzung der Rogue Client Detection ist **keine** Konfiguration der LANCOM Wireless Router erforderlich.

Folgende Gruppen nutzt der WLANmonitor zur Sortierung der gefundenen Clients:

- Alle Clients: Auflistung aller gesehener Clients der folgenden Gruppen (die Clients werden entsprechend der Gruppe farblich dargestellt)
- Neue Clients: neue unbekannte Clients gelangen automatisch in diese Gruppe (die Clients werden gelb dargestellt)
- Rogue Clients: Clients, die als Rogue erkannt und dringend zu beobachten sind (die Clients werden rot dargestellt)
- Unbekannte Clients: Clients, bei denen weitere Untersuchungen notwendig sind (die Clients werden grau dargestellt)
- Bekannte Clients: Clients, die keine Gefahr darstellen (die Clients werden grau dargestellt)
- Eigene Clients: neue eigene Clients, die bei Access Points assoziiert sind, die der WLANmonitor beobachtet, gelangen automatisch in diese Gruppe (die Clients werden grün dargestellt)

Die gefundenen Clients können je nach Status in eine entsprechende Gruppe verschoben werden. Innerhalb der einzelnen Gruppen können über das Kontextmenü (rechte Maustaste) eigene Gruppen angelegt werden (ausgenommen der Gruppe 'Alle Clients').

LANCOM Systems

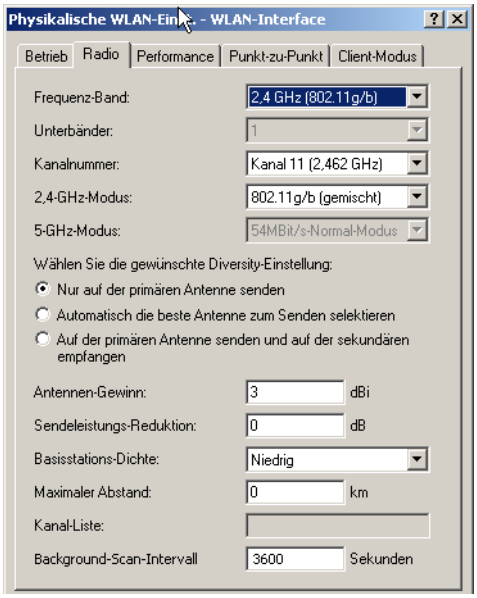
LANCOM™ Techpaper
Rogue AP und Rogue Client Detection

Background WLAN Scanning

Zur Erkennung anderer Access Points in der eigenen Funkreichweite können LANCOM Wireless Router die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der Access Points abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Die Informationen über die gefundenen Access Points können im WLANmonitor oder in der Statistik des LANCOM Wireless Router eingesehen werden.

Zur Konfiguration des Background-Scans wird eine Zeit angegeben, innerhalb der alle verfügbaren WLAN-Kanäle einmal auf die empfangenen Beacons hin gescannt werden sollen (Background-Scan-Intervall).



Um Beeinträchtigungen der Datenübertragungsrate zu verhindern, beträgt das Intervall zwischen den einzelnen Kanal-Scans mindestens 20 Sekunden. Kleinere Eingaben werden automatisch auf dieses Mindestintervall korrigiert. Zum Beispiel wird bei 13 zu scannenden Funkkanälen im 2,4 GHz-Band das gesamte Spektrum minimal innerhalb von 13 x 20s = 260 Sekunden einmal gescannt.

Das Background-Scanning kann auf eine geringere Anzahl von Kanälen beschränkt werden, wenn der Indoor-Modus aktiviert wird oder wenn in der Kanal-Liste die erlaubten Kanäle angegeben werden.

© 2006 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten. **LANCOM**, **LANCOM Systems**, **LCOS** und **LANvantage** sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Änderungen vorbehalten. Keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. Version 1.0

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de I Internet www.lancom.de

LANCOM Systems