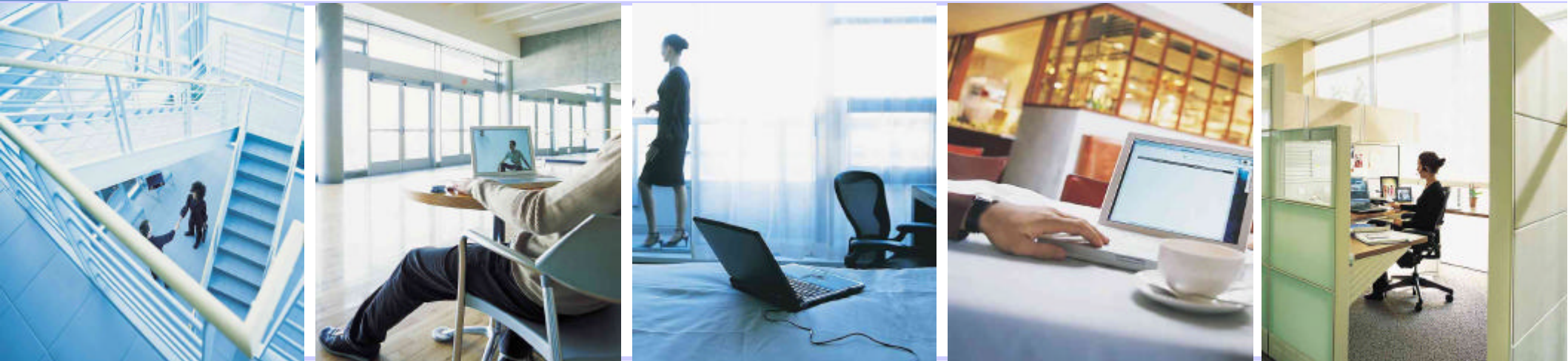


LANCOM Systems

... connecting your business



LANCOM Software Version 3.50

August 2004

LC.OS 3.50
[LANCOM OPERATING SYSTEM]

© 2004, LANCOM Systems GmbH

www.lancom.de

LANCOM
Systems

Inhalt

Auf den folgenden Seiten möchten wir Ihnen einen Überblick über die neuen Features und Verbesserungen der neuen LCOS-Version und der LANtools geben.

Die Themen im Detail:

- ▶ Die neue LCOS-Version 3.50
- ▶ 802.11i mit LANCOM Wireless Geräten
- ▶ 802.11i mit AirLancer Client Adaptern
- ▶ Hinweise zu Service und Support

Informationen über Features der vorausgegangenen LCOS-Versionen finden Sie im [Dokumentationsteil](#) der LANCOM CD.

Die neue LCOS-Version 3.50

- ▶ Unterstützt alle LANCOM Modelle.
- ▶ Auch für Telekom Business LAN
- ▶ kompatibel zu AirLancer MC-54g/ag, PCI-54ag mit Treiber Version 3.1. und höher

Highlights:

Einführung neuer Sicherheitsstandards für Wireless LAN:

- ▶ WPA
- ▶ 802.11i
- ▶ Neues LANCOM Referenzhandbuch

Neue Sicherheitsstandards für Wireless LAN

Hardware-AES-Verschlüsselung ist integriert in LANCOM

L-54g/ag, 1511, 1521, 1811, 1821, 3550, 3050 (nur mit externer AirLancer MC-54g/ag)

und in den AirLancer MC-54g und AirLancer MC-54g sowie AirLancer PCI-54g Client Adaptern

- ▶ 802.11i mit Passphrase für alle 54MBit/s Wireless Produkte
- ▶ Maximale Sicherheit und Performance durch integrierte Hardware-AES-Verschlüsselung

Zitat Heise Ticker (c't): *„Der nun ratifizierte Standard IEEE 802.11i umfasst alle Fähigkeiten von WPA und ergänzt diese durch die Vorschriften für die Verwendung des Advanced Encryption Standard (AES) zur Verschlüsselung von Daten. Der AES bietet genügend Sicherheit, um die notwendigen Spezifikationen des Federal Information Standards (FIPS) 140-2 einzuhalten, die von vielen staatlichen Stellen gefordert werden.“*



802.11i
Enhanced Security mit AES
Hardware-Verschlüsselung

IEEE 802.11i – die Komponenten

Die Basis: WPA (WiFi Protected Access)

- ▶ Verschlüsselungsverfahren: TKIP, MIC („Michael“)
- ▶ Hauptanwendung: mit Passphrase (Pre-Shared-Key)
 - ▶ Komfortablere Einrichtung als ein WEP-Hex-Schlüssel durch Angabe eines einfachen ASCII-Strings mit 8-63 Zeichen.

Der neue Standard: IEEE 802.11i

- ▶ Entspricht WPA + AES Verschlüsselung
- ▶ Abwärtskompatibilität zu WPA/TKIP (schaltbar)
- ▶ AirLancer 54 Clients verschlüsseln AES in Hardware ohne Performance-Einbußen (AirLancer MC-54g/ag und PCI-54ag)

IEEE 802.11i – die Vorteile

Optimales Sicherheitslevel

- ▶ Mit AES Verschlüsselung State-Of-The-Art wie bei VPN
- ▶ Keine offenen Sicherheitslücken mehr

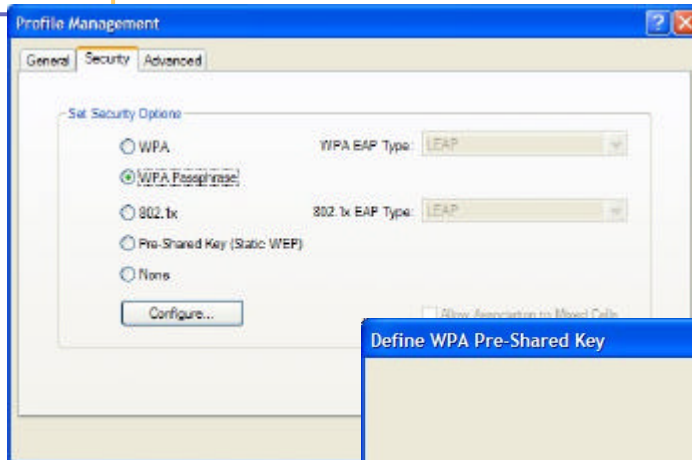
Einfach einzurichten

- ▶ Mit Passphrase reicht die Angabe eines einfachen ASCII-Strings (8-63 Zeichen)
- ▶ Der Verschlüsselungs-Key wird daraus automatisch errechnet
- ▶ Sicherheit durch regelmäßigen automatischen Key-Wechsel

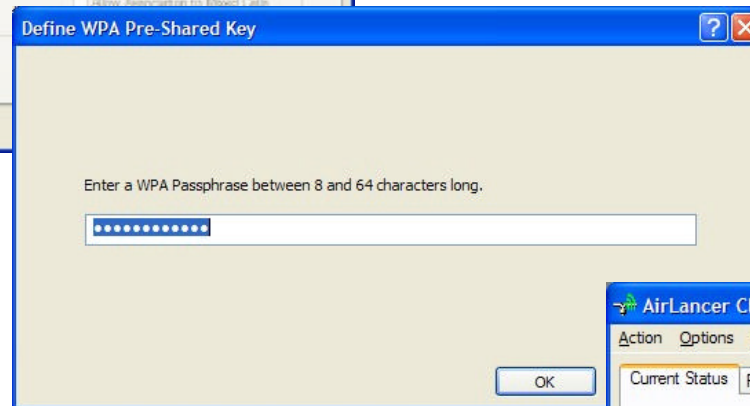
WEP vs. IEEE 802.11i/WPA

	WEP	WPA	802.11i
Verschlüsselung	Benutzt ‚weiche‘ Keys. Kann mit Tools in kurzer Zeit geknackt werden.	Mit TKIP und MIC bessere Verschlüsselung. Theoretische Zeit bis zur Schlüsselwiederholung sehr lang.	Mit AES gleichwertige Sicherheit wie VPN.
	40bit/104bit/128bit RC4	128bit RC4	128bit AES
	Key-Verteilung per Hand, Man-in-the-middle Attacke möglich	Durch Passphrase automatische Keyberechnung	Automatische Keyberechnung, AES in Hardware
Authentifizierung	keine	4-Wege-Handshake mit Session- und Group-Key	4-Wege-Handshake mit Session- und Group-Key

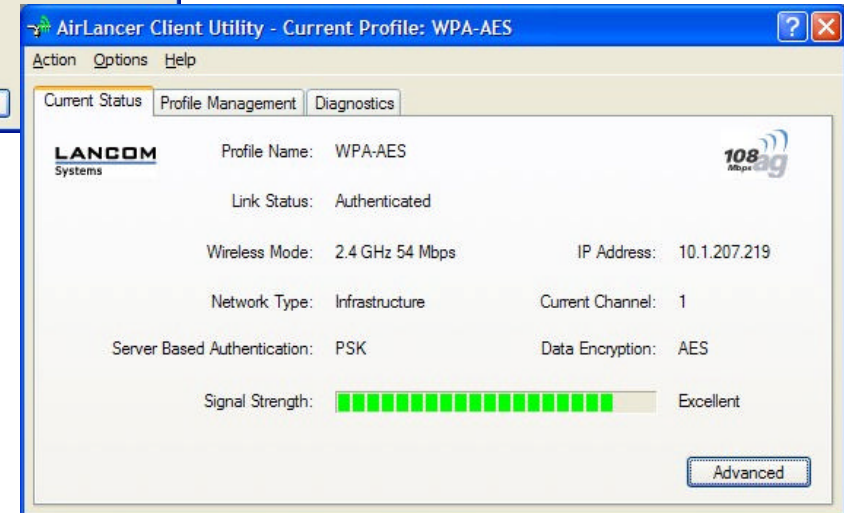
AirLancer Client Adapter Version 3.1.



1.: WPA Passphrase auswählen



2.: WPA Passphrase eingeben



3.: PSK+AES=802.11i funktioniert!

► Die Treiber für
AirLancer 54
Client Adapter
sind auf
www.lancom.de
zum Download
verfügbar

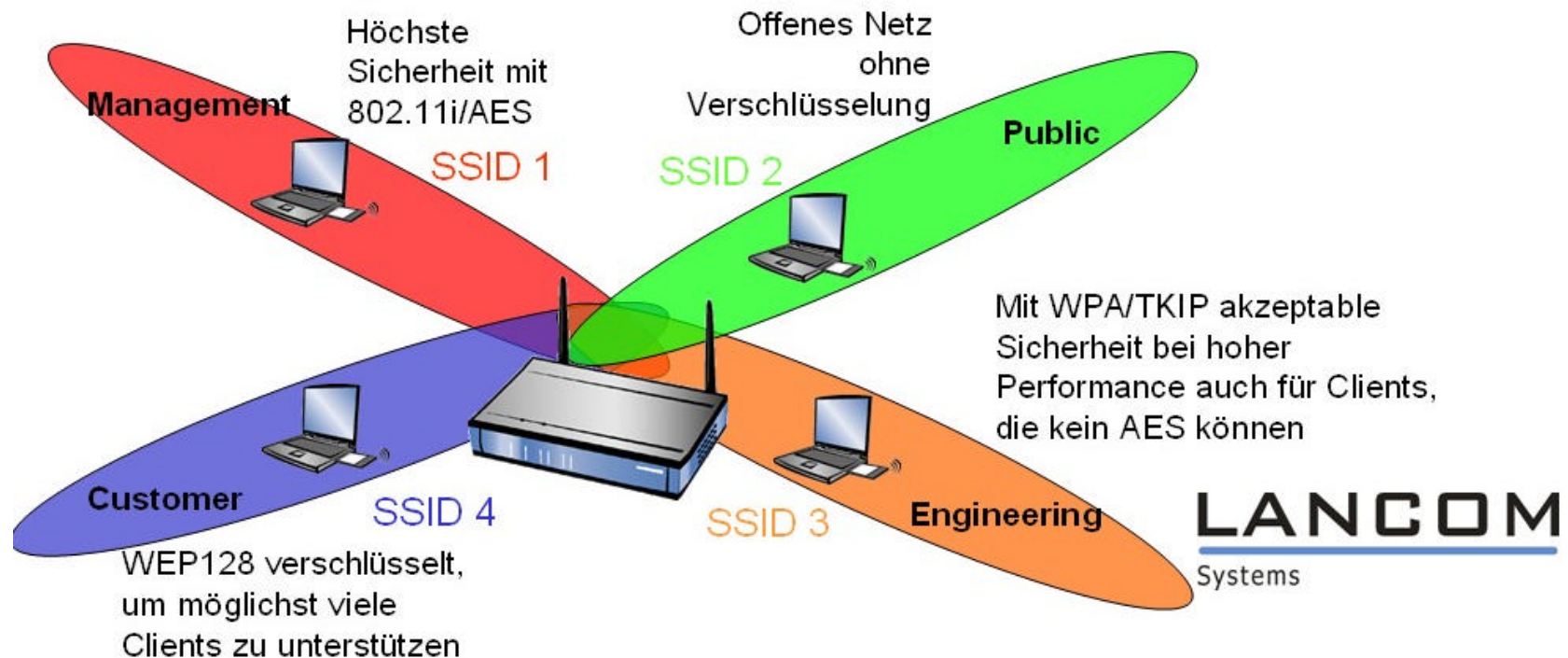
Migration von WEP → WPA → 802.11i

Mit der Möglichkeit, pro Wireless-Interface 8 WLAN-Netzwerke mit jeweils unterschiedlichen Sicherheitsmethoden zu versehen, kann der Betreiber eines WLAN-Netzes jedem Nutzer die Sicherheit bieten, die sein Client unterstützt. So können in einem Netz die Clients arbeiten, die WEP benötigen, während die Nutzer, die die höchste Sicherheitsstufe mit AES exklusiv benötigen, ein eigenes Netz mit 802.11i bereitgestellt bekommen. Unterstützt werden kann dies noch durch ein VLAN-Tagging, um die Nutzergruppen auch in der dahinterliegenden Infrastruktur entsprechend ihrer Sicherheitsstufe zuordnen zu können.

Techpaper zu

- ▶ 802.11i,
 - ▶ Multi SSID
- und
- ▶ 108 MBit/s
- sind unter

www.lancom.de
zum Download
verfügbar



IEEE 802.11i – die Highlights

IEEE 802.11i

- ▶ Der lange erwartete Sicherheitsstandard
- ▶ Volle Geschwindigkeit mit Hardware-AES
- ▶ Einfache Benutzung
- ▶ Schließt alle bekannten Sicherheitslücken
- ▶ Unterstützt WDS (Wireless P2MP, P2Station, Client Mode)

Ausblick

- ▶ 802.11i mit 802.1x ab LCOS Version 4
- ▶ P2P-Unterstützung für 802.11i/WPA ab LCOS Version 4

Referenzhandbuch

LANCOM Referenzhandbuch neu aufgelegt

- ▶ mehr als 300 Seiten Hintergrundinformationen, Praxistipps und detaillierte Beschreibungen aller Funktionen
- ▶ Überarbeitete Kapitel:
 - ▶ Wireless LAN mit 802.11i und WPA/TKIP
 - ▶ Als PDF im [Download-Bereich](#) und auf der [LANCOM CD](#)

LANCOM Systems

... connecting your business

LCOS 3.50
[LANCOM OPERATING SYSTEM]

Sonstige Änderungen

Die vollständige, **detaillierte Änderungshistorie** finden Sie zusammen mit anderen Dokumenten, LCOS-Versionen und LANtools im Internet:

▶ www.lancom.de/download

LANCOM
Systems

Service und Support

Wir wünschen Ihnen viel Erfolg mit Ihrem neuen LANCOM Produkt!

Über **Lob und Kritik, Anregungen oder Fragen** freuen wir uns unter info@lancom.de.

Aktuelle Informationen zu Service und Support entnehmen Sie bitte unserem Support-Beileger, unseren Internetseiten oder unserer Wissensdatenbank (**Knowledge Base**) unter www.lancom.de/support.

Sollten Sie trotz Handbuch und unseren aktuellen Support-Themen im Internet einmal nicht weiter wissen, so steht Ihnen in Deutschland werktags von 9.00-17.00h unsere **Support-Hotline** unter 0190-764100 (1,24€/ Min.) zur Verfügung.

Ihr LANCOM Systems Team.



LANCOM

Systems

LANCOM
Systems