



Die Wireless Innovation: Mehr Sicherheit durch neue Generation von Cisco Access Points



Wolfram Maag

Consulting Systems Engineer Mobility

Session Objectives

- Nach dem Webinar sollen Sie die Vorteile von 802.11n für Ihr Netz verstehen und den Nutzen vom AP1140 kennen.
- Sie sollen das Potential einer WIPS Lösung kennen und dieses Experten Know-How im eigenen Netzwerk nutzen lernen

Agenda

- Wireless LAN als Business Tool
- Wireless Intrusion Prevention
- Stabileres Funkfeld durch 802.11n

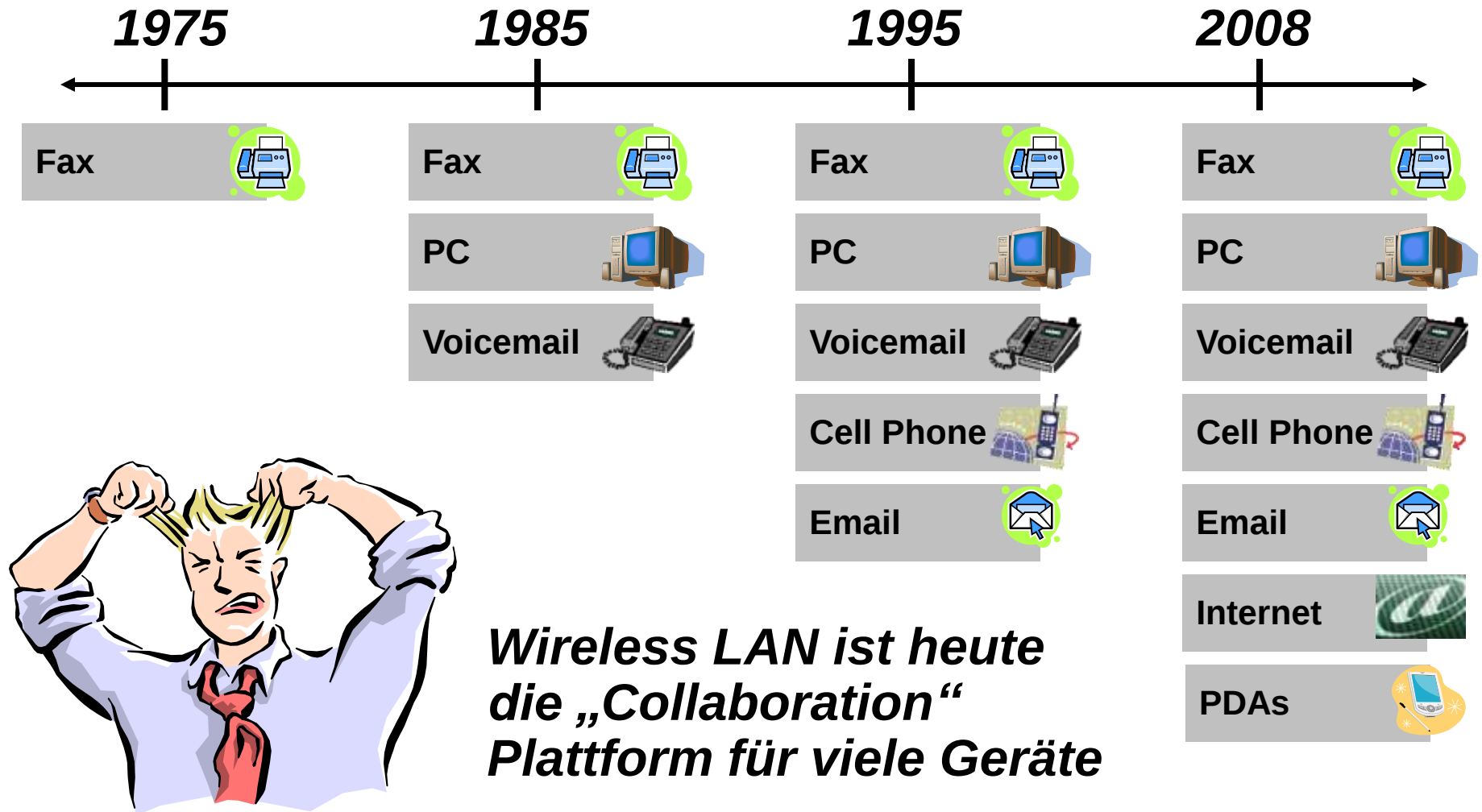




Wireless LAN als Business-Tool



Wireless LAN ist ein Business Tool



Mobility wächst

Viele Geräte verfügen nur noch über WLAN Interfaces oder nutzen WLAN als primäres Netzzugangs-Medium ... und es werden immer mehr!



Aspire One

You are here: [Home](#) / [Products & Services](#) / [Tablet PCs](#) / [Aspire One](#)

Acer recommends Windows® XP Professional.



Acer redefines mobile computing with fun and powerful computing.

SmartStart in just 15 sec
From the moment you switch on, the Aspire One is ready to go. With its simple, intuitive interface, you can get up and online in just 15 seconds. The Aspire One is as unique as the user, so that it's just right for your life with the Aspire One.

Was sind also die Requirements

- Kompatibilität
- Maximale Sicherheit
- Hohe Bandbreiten
- Einfache Administration / geringe Administrationskosten



Kompatibilität

- CCX – Cisco Compatible Extensions

Funktionserweiterung bei den Clients

Getestete Interoperabilität

95% der Hardware unterstützt CCX

Verschiedene Versionen mit unterschiedlichen Features



- Wi-Fi Zertifizierungen

- Assurewave Program – Post Release Programm



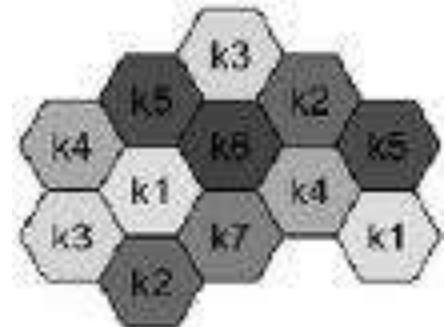
Maximale Sicherheit



- Sichere Datenübertragung
 - WPA v1/v2
 - EAP- Authentifizierung
- Sichere Infrastruktur
 - Authentifizierung der AP's am Netzwerk und Controller
 - „Tunneled“ Übertragung
- Auf Angriffe achten
 - Funkstörungen erkennen und vermeiden: RRM
 - Integrierte IDS / wIPS auf MSE
- Abwehr Maßnahmen:
 - Management Frame Protection
 - Containment

Hohe Bandbreite & einfache Administration

- 802.11n verbessert dramatisch die Übertragungsleistungen
- Radio Ressource Management übernimmt die Frequenzplanung
- Vermeidung gestörter Frequenzen
- Optimierte Verteilung im Gesamtsystem
- Reporting von Änderungen



WLAN liefert auch neue Services!

- Zusätzlich zum Netzwerk Access werden aber weitere Dienste angeboten

Guest Access

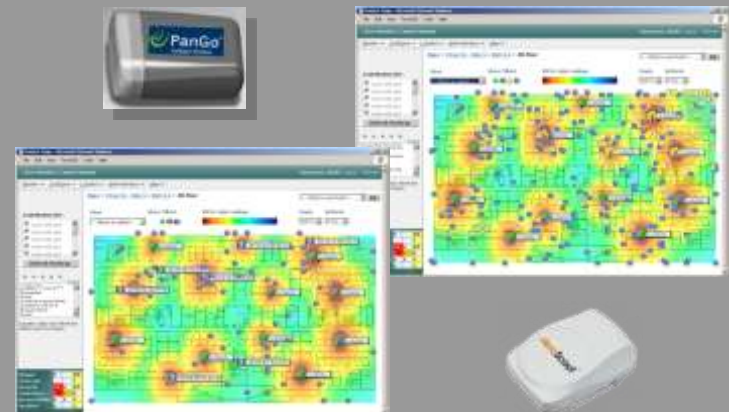


Voice

- WiFi enabled voice
- 792x, Dualmode
- Ablösung von DECT
- ein Netz für alle Services



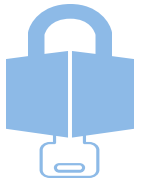
Location





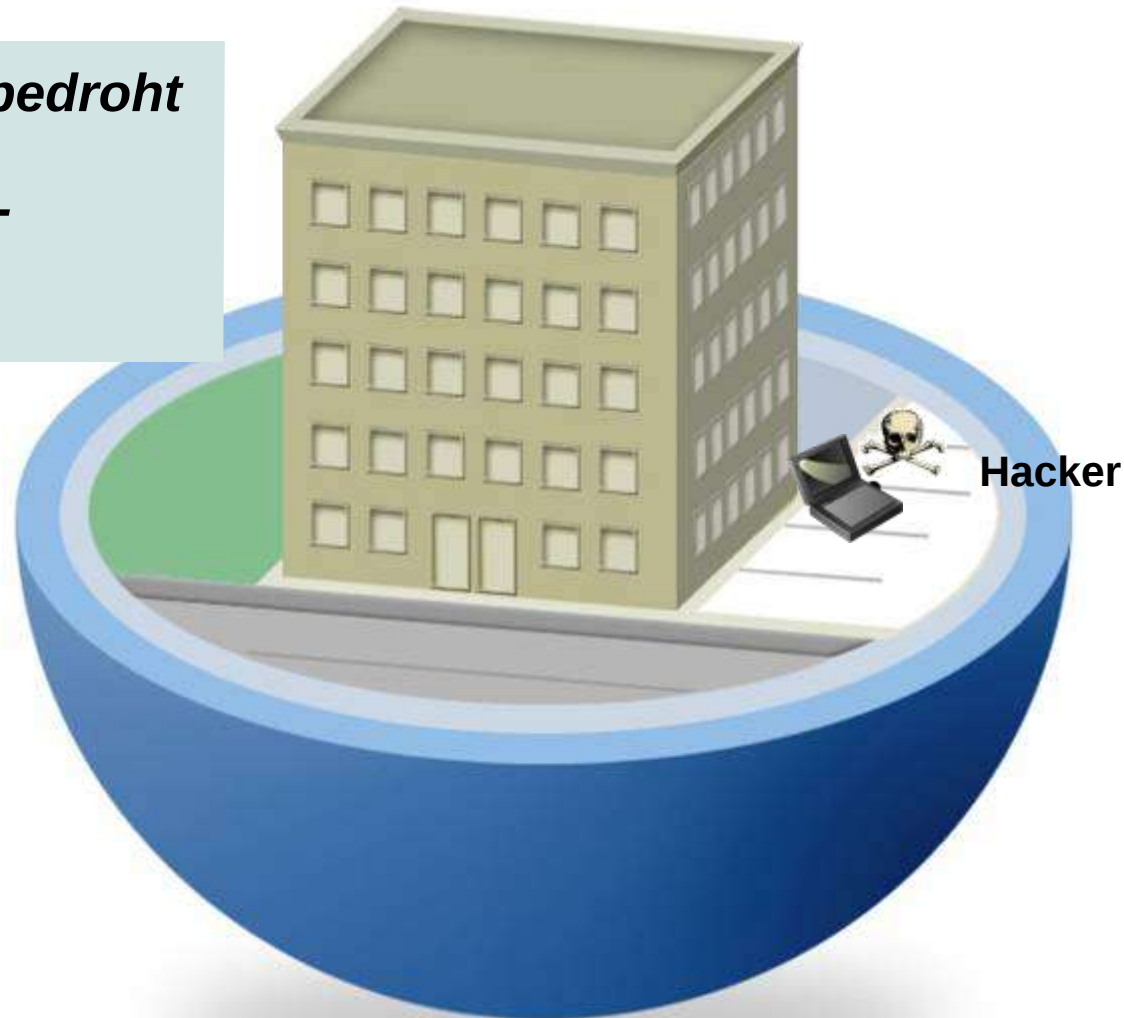
wIPS: Wireless Intrusion Prevention





Angriffen können von überall kommen

***Ein Rogue AP bedroht
die komplette
Unternehmens-
sicherheit***



*Integrierte Controller Security bietet guten Schutz
WIPS bietet zusätzliches Expertenwissen*

Sicherheit: Client Verschlüsselung

- Alle relevanten Varianten werden angeboten
- WPA und WPA2?
 - Authentication und Encryption Standards für Wi-Fi Clients und APs
 - 802.1x Authentifizierung
 - WPA nutzt TKIP Encryption
 - WPA2 nutzt AES Block Cipher Encryption
- Was soll ich nehmen?
 - Gold, für System die das supporten (NIC/Oss)
 - Silver, für älterer Clients
 - Bronze, wenn es keine andere Möglichkeit gibt (z.B. ASDs)
 - Unencrypted für Guest Access



Gold

WPA2/802.11i

- EAP-Fast
- AES



Silver

WPA

- EAP-Fast
- TKIP

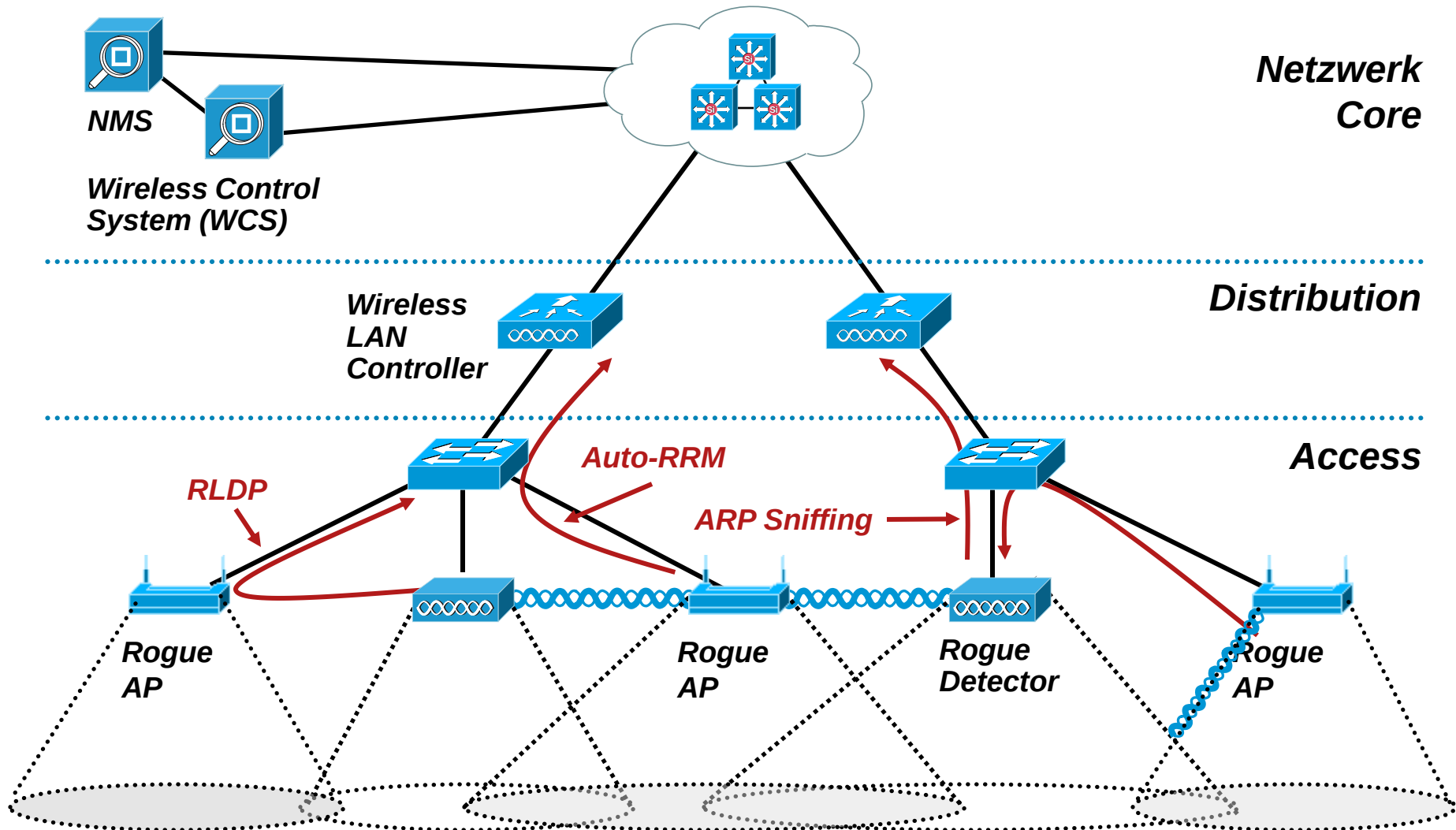


Bronze

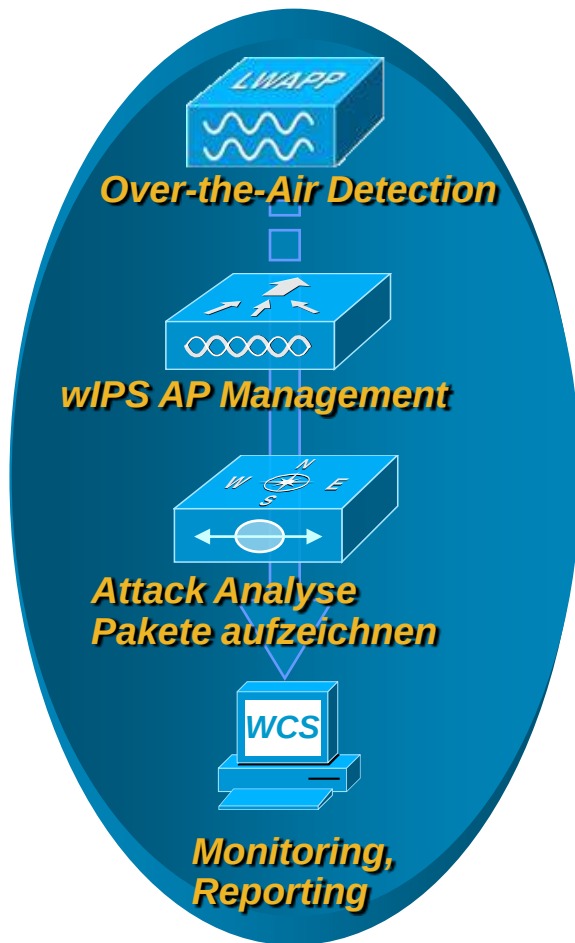
Dynamic WEP

- EAP-Fast/LEAP
- VLANs + ACLs

Monitoring und Rogue Detection



wIPS Komponenten



- wIPS Monitor Mode AP – zur Erkennung von Angriffen
- Controller – managed wIPS APs, leitet wIPS Daten an MSE weiter
- MSE 3310 mit Aggregation, Analyse der Daten, Aufzeichnung
- WCS – zentrale Konfiguration und Monitoring

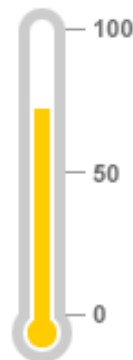
wIPS Alarms and Security Dashboard

Security			
Summary			
Malicious Rogue APs			
Friendly Rogue APs			
Unclassified Rogue APs			
Adhoc Rogues			
Rogue Clients			
Shunned Clients			
Alarms Summary			
Malicious	0	0	0
Unclassified	0	0	301
Coverage Hole	0	0	0
Security	3	17	0
Controllers	1	0	1
Access Points	7	0	5
Mobility	0	0	2
Mesh Links	0	0	0

**wIPS Alarm
under
"Security"**

Security Summary

Security
Index : 71.12



Top Security Issues | [View All](#) | [Devices](#)

- Check for all Standard and Custom Signatures disabled for a Controller. (1)
- Interface set to management for WLAN. (1)
- Protection Type set to None for a Controller. (1)
- SNMP V1 or V2 with default Community for a Controller. (1)
- MFP Client Protection set to Optional for WLAN. (1)

** Note that Security Index is calculated as*

**wIPS
Denial of
Service
Alarme**

Threats And Attacks | [View All](#)

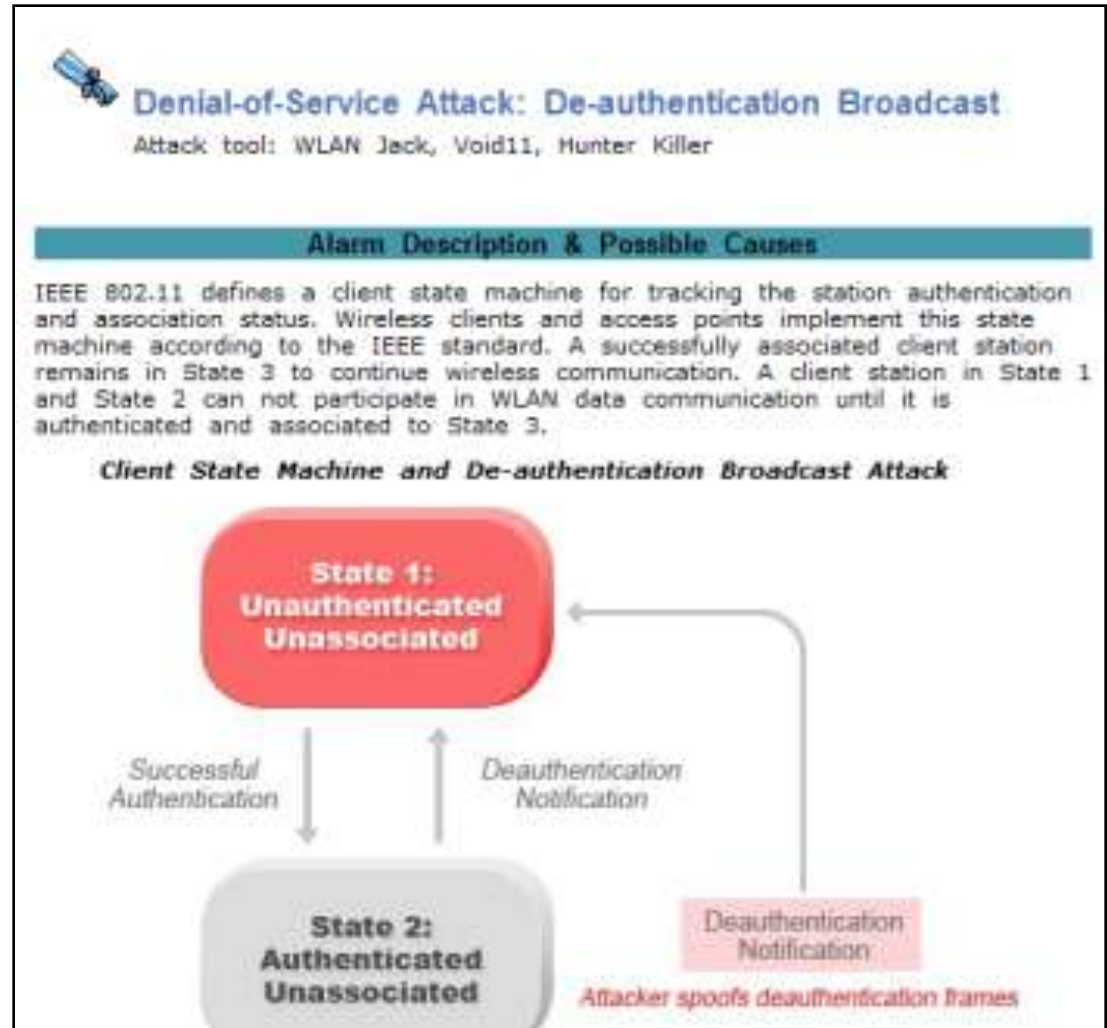
wIPS Denial of Service Attacks	Last Hour	24 Hours	Total Active
DoS: De-Auth broadcast attack	0	1	<u>1</u>
DoS: RF jamming attack	0	1	<u>1</u>

wIPS Security Penetration Attacks	Last	24	Total Active
Fake APs detected	0	0	<u>1</u>
Unauthorized association by vendor list	0	0	<u>1</u>
ChopChop Attack	0	0	<u>2</u>
Soft AP or Host AP detected	0	0	<u>14</u>

**wIPS
Penetration
Alarme**

wIPS Beschreibung der Angriffe

- Verfügbar für jeden Alarm
- Per Click auf “Help” sofort einsehbar



Datenaufzeichnung

- konfigurierbar je Angriffsvariante
- Angriff kann komplett mitgeschnitten werden
- .cap Datei der Pakete Wireshark, Omnipcap, etc.
- Gespeichert auf der MSE

[Alarm](#) > [Events](#) > WIPS AP '1240-mon'

General

Forensic_001D4523D5A0_5.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
3416	3.060999		IntelCor_89:ef:38	IEEE 8	Clear-to-send
3417	3.063000		Cisco_a6:f4:70 (RA	IEEE 8	Clear-to-send
3418	3.064000		Cisco_a6:f4:70 (RA	IEEE 8	Clear-to-send
3419	3.065999	00:1c:b1:8b:db:51	Broadcast	IEEE 8	Beacon frame, s
3420	3.068000	Cisco_a8:d2:10	Broadcast	IEEE 8	Beacon frame, s
3421	3.071000	Cisco_a8:d3:20	Broadcast	IEEE 8	Beacon frame, s
3422	3.072999	00:1d:46:7e:c7:91	Broadcast	IEEE 8	Beacon frame, s
3423	3.072999		IntelCor_89:ef:38	IEEE 8	Clear-to-send
3424	3.072999		IntelCor_89:ef:38	IEEE 8	Acknowledgement
3425	3.076000	Cisco_a8:d2:18	Broadcast	IEEE 8	Beacon frame, s

Frame 3417 (10 bytes on wire, 10 bytes captured)

IEEE 802.11

Data Rate: 11.0 Mb/s
Channel: 6
Signal Strength: 71%

Type/Subtype: Clear-to-send (28)

Frame Control: 0x00C4 (Normal)
Duration: 44
Receiver address: Cisco_a6:f4:70 (00:17:df:a6:f4:70)

Type and subtype combined (wlan.fc.type_subtype), 1 byte | P: 4075 D: 4075 M: 0

MSE

Controller MAC

WIPS AP MAC 00:1d:46:7e:c7:91

Forensic File **Forensic_001D4523D5A0_5.cap**



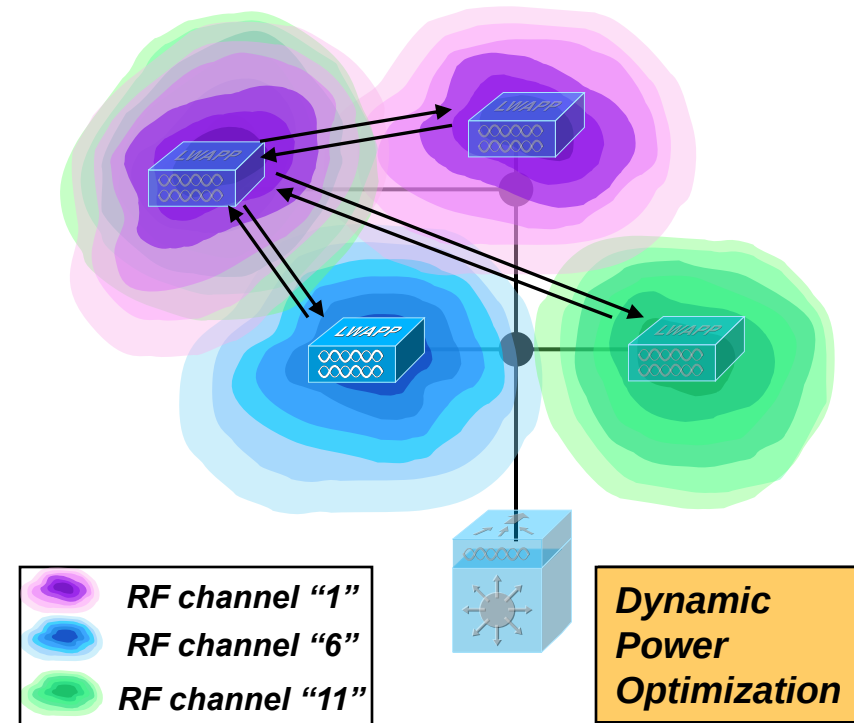
Stabileres Funkfeld durch 802.11n



Radio Resource Management

Real-Time RF Management

- RF Umgebung ist nicht konstant, Controller übernehmen Regelung
- Der Controller hat einen Gesamtüberblick über das Netz und optimiert die einzelnen AP's
- dauerhafte Störungen werden in die Kalkulation mit einbezogen



Benefits

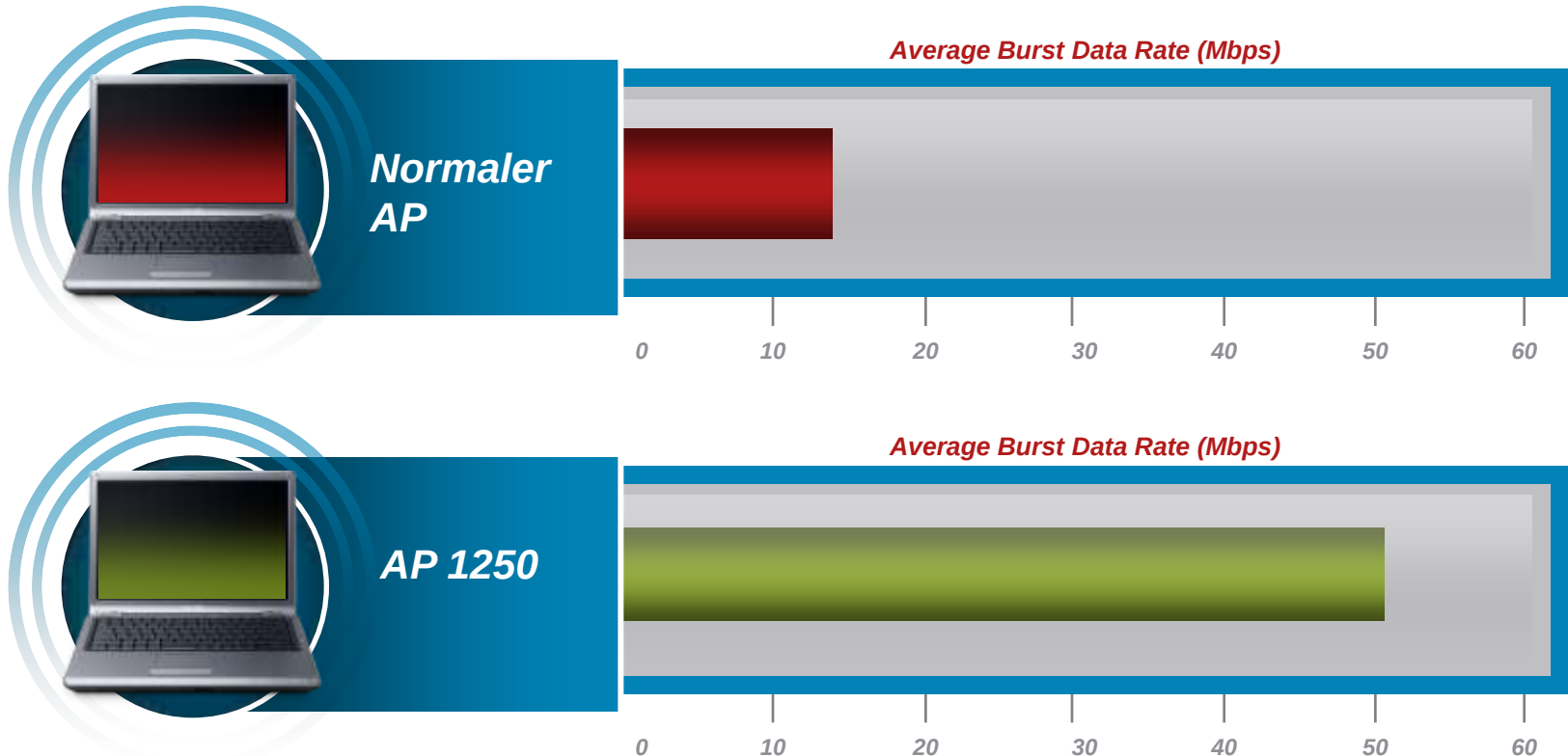
- *optimierte RF Umgebung erlauben bessere Zuverlässigkeit und höhere Performance*
- *Komplettes RF Management ohne spezielles KnowHow*
- *Keine permanente RF Re-Kalibrierung erforderlich*

802.11n: Zuverlässigere Abdeckung

- Höherer mittlerer Durchsatz, zuverlässigere Bedingungen für alle Clients

höhere Zuverlässigkeit, bessere Nutzer Erfahrung

Vorhersehbarer Durchsatz auch in schwierigen Situationen



Erprobte Plattform für Mobile Access

Indoor Access Points



1130AG



1140 N

Indoor Rugged Access Points



1240AG



AP1250

Outdoor Access Points/Bridges



1520



1300

Access Points

Features

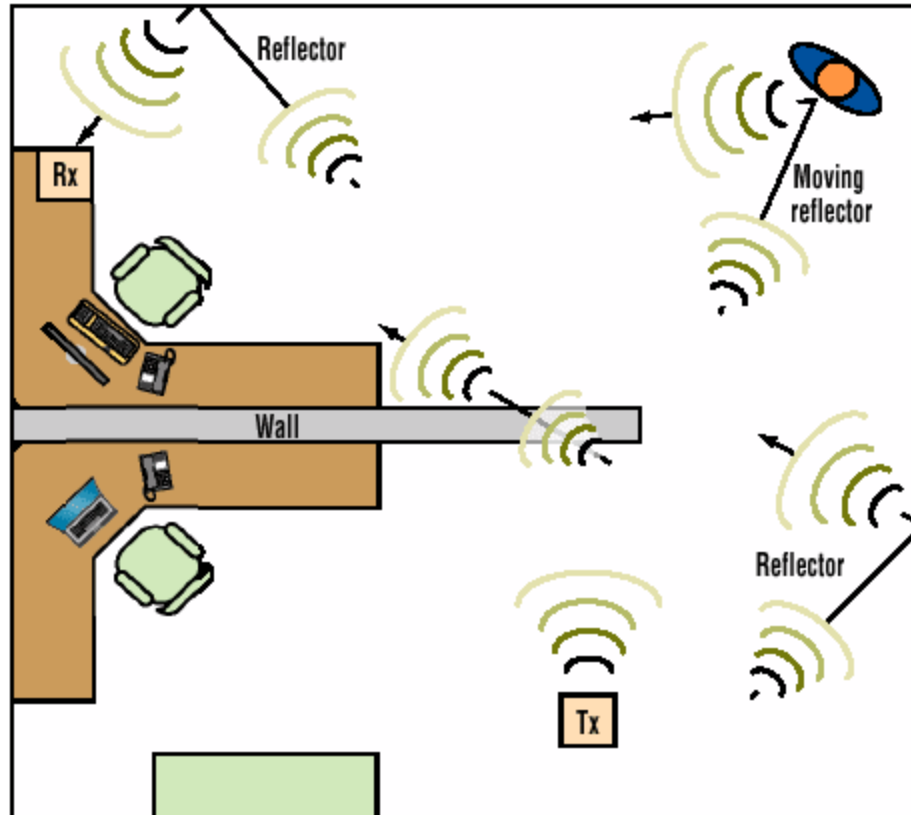
- *beste Reichweiten und Durchsatz*
- *Enterprise Class Security*
- *Viele Konfigurationsoptionen / Flexibilität*
- *Simultanes Air Monitoring und Datenverkehr*

Vorteile

- *Zero Touch Management*
- *Für alle Deployment Szenarien (Indoor und Outdoor)*
- *Services von sicherer Coverage bis advanced Services*
- *Vielzahl unterstützter Antennen*

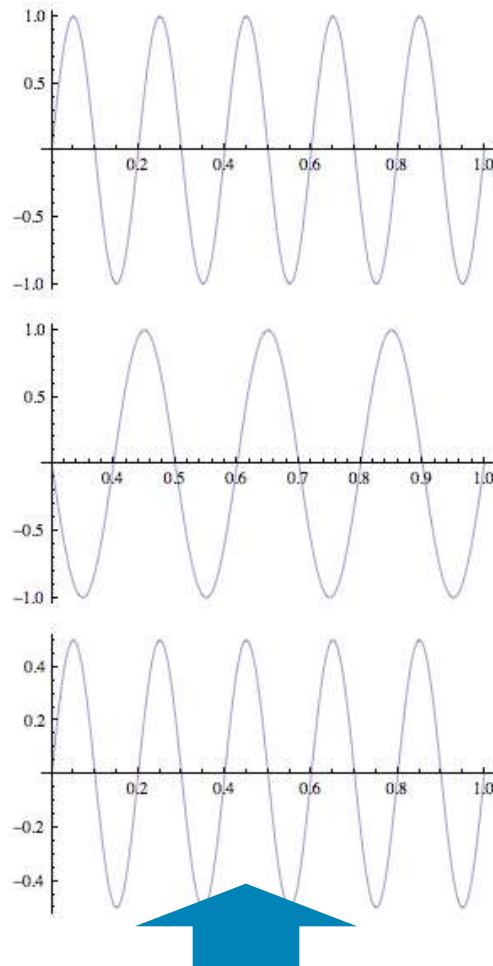
MIMO – Multi Inputs, multiple Outputs

- MIMO nutzt Reflektionen

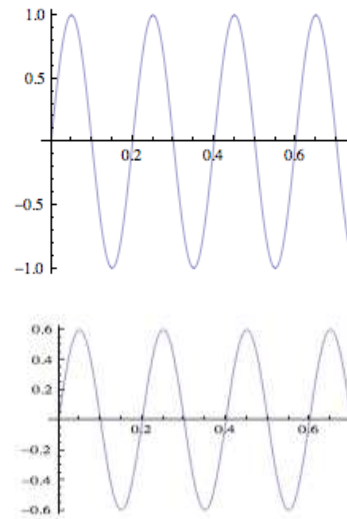


***Reflexionen in einer normalen Büroumgebung
- aber auch unter schwierigen Umständen***

Multipath Reflektionen bei einem SISO AP

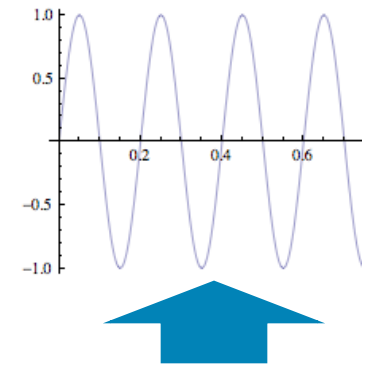
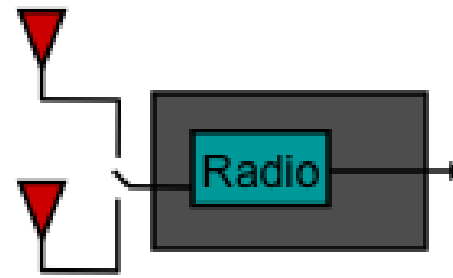


**Multipath Reflektionen
des Original Signals**



**Signal, das die
Antennen sehen**

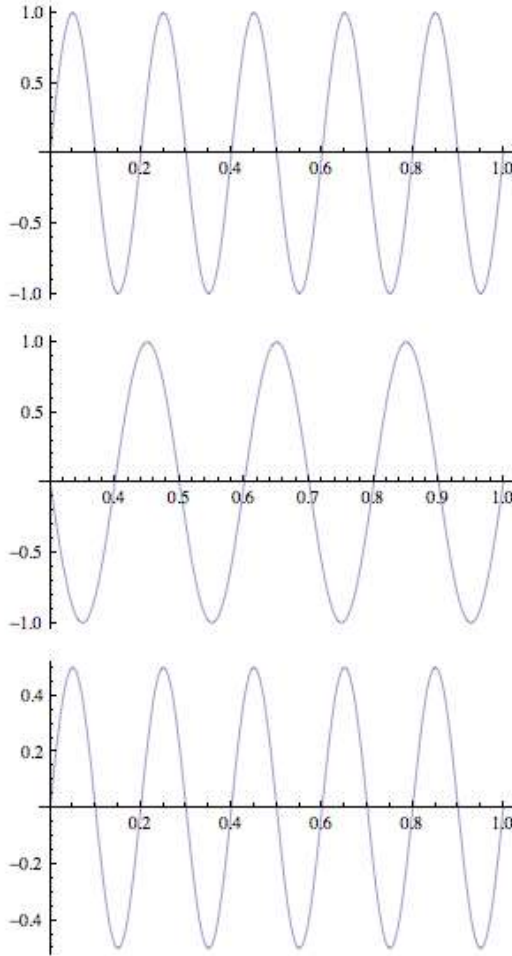
**SISO = Single Input,
Single Output**



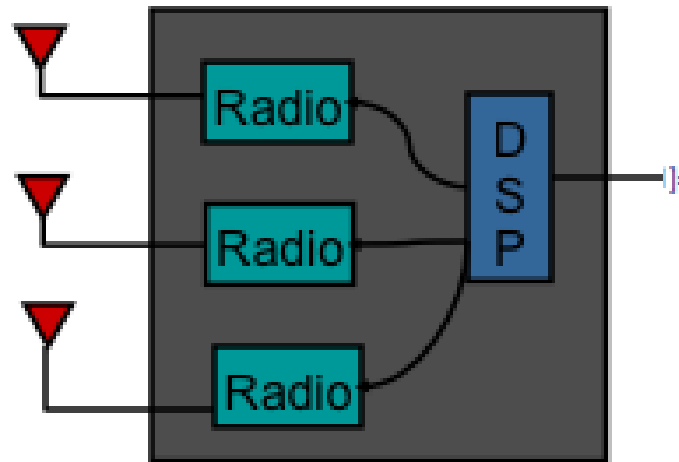
**Radio nimmt das
stärkste Signal**

Multipath Reflektionen bei einem MIMO AP

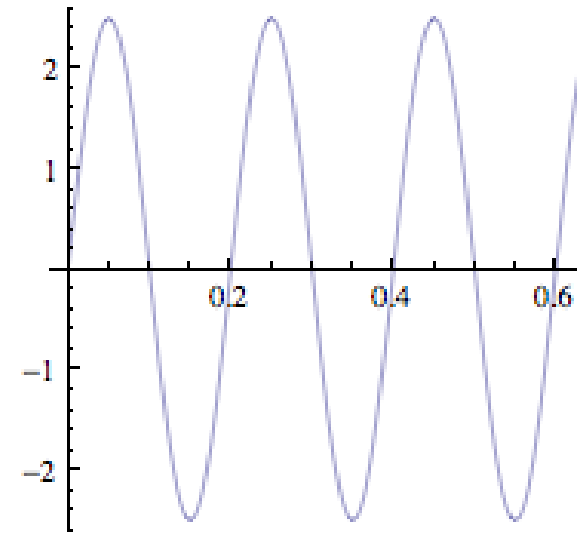
MIMO = Multiple Input,
Multiple Output



***Multipath Reflektionen
des Original Signals***



***DSP korrigiert und
addiert das Signal***



***Resultat ist deutlich
stärker***

Aironet AP 1250 Access Point

- Mehr Durchsatz
 - Schnelle CPU für mehr Datendurchsatz
 - 10/100/1000 Ethernet Port
- Mehr Memory für erweiterte Features
- Als Controller basierender oder Autonomer AP erhältlich
- 802.11n AP im WiFi Testfeld



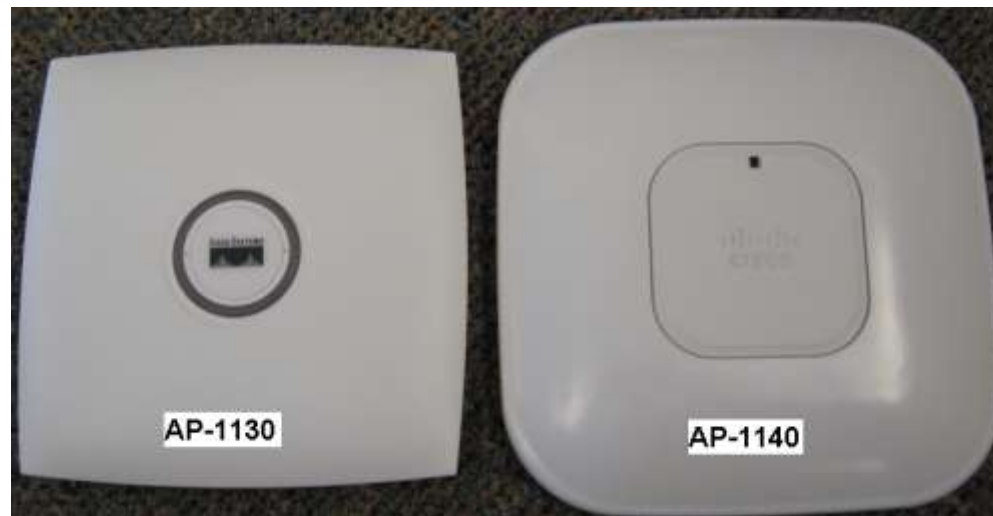
Aironet AP 1140

- Aironet AP-1140 ist für den Bürobereich geeignet
 - 5 GHz 802.11a/n
 - 2.4 GHz 802.11b/g/n
 - integrierte Antennen
 - unauffällige Bauform
- Designed für volle 802.11n Features mit 802.3af Power
- Gleiche Funktionen wie AP1250



Vergleich AP1130 und AP1140

- Upgrade von AP1130 nach AP1140 ohne Werkzeug
- Attraktive Trade-Ins für alte Komponenten



Zusammenfassung

- Cisco bietet im Bereich Übertragungs- und Störsicherheit wesentliche Verbesserungen
- Nutzen Sie die Expertise im WIPS
- 802.11n eröffnet Ihnen den Weg zu einem sehr stabilen WLAN Netz



