

# **Wireless LAN Evaluierung**

## **Arbeitsweise, Varianten, Schwachstellen, Planung, Installation**

**von**

**Dipl.-Math. Cornelius Höchel-Winter**

mit Einzelbeiträgen von

Mark Groten  
Dr. Simon Hoff  
Dipl.-Inform. Gaby van Laak  
Dr. Joachim Wetzlar

## Inhaltsverzeichnis

<b><u>INHALTSVERZEICHNIS</u></b>		<b><u>I</u></b>
<b><u>1</u></b>	<b><u>EINFÜHRUNG</u></b>	<b><u>1</u></b>
<b><u>2</u></b>	<b><u>TYPISCHE ANWENDUNGSGEBIETE</u></b>	<b><u>5</u></b>
2.1	LAN-Erweiterung im Büroumfeld	5
2.2	Notebook-Einbindung	6
2.3	Konferenz und Messestand	6
2.4	Kaufhäuser	7
2.5	Krankenhäuser	7
2.6	Hot Spots	7
2.7	LAN-Koppelung	7
2.8	Entscheidungskriterien	8
<b><u>3</u></b>	<b><u>GRUNDLAGEN VON FUNKTECHNIKEN</u></b>	<b><u>10</u></b>
3.1	Frequenzbänder	10
3.2	Ausbreitung elektromagnetischer Wellen	13
3.2.1	Dämpfungsverluste	14
3.2.2	Polarisation	17
3.3	Interferenzen	19
3.3.1	Rauschen	20
3.3.2	Systemfremde Interferenzen	21
3.3.3	Systemeigene Interferenzen	24
3.3.4	Mehrwegeausbreitung	27
3.3.5	Konsequenzen	31
3.4	Modulationsverfahren	32
3.4.1	Spread-Spectrum-Technik	38
3.4.2	Multiplexing und Multiple Access	44
3.5	Anforderungen an eine Funk-LAN-Technik	48
3.6	Funkstandards	49



5.4.3	Extended High Rates nach 802.11g	100
5.4.4	Interoperabilität zwischen 802.11b und 802.11g	102
5.4.5	Rate Selection	104
5.4.6	Frameformate	109
5.4.7	OFDM nach 802.11a	113
5.4.8	TPC und DFS nach 802.11h	115
5.4.9	Frequency Hopping Spread Spectrum (FHSS)	118
5.4.10	Vergleich DSSS vs. FHSS	121
5.4.11	Infrarot Schnittstelle	123
5.5	Technik (MAC-Layer)	126
5.5.1	Frameformate	127
5.5.2	Distribution Coordination Function (DCF)	130
5.5.3	Point Coordination Function (PCF)	134
5.5.4	802.11e	136
5.5.5	Acknowledgement und Retransmission	138
5.5.6	RTS/CTS – Virtual Carrier Sense	140
5.5.7	Fragmentierung	144
5.5.8	Beacons, Verwaltungsinstanzen im WLAN	148
5.5.9	Powermanagement	151
5.5.10	Die Verwaltung von Wireless LANs: Scanning, Authentication und Association	153
5.5.11	Roaming	161
5.6	Inter-Access Point Protocol (802.11F)	164
<b>6</b>	<b>SICHERHEIT IN WLANS</b>	<b>168</b>
6.1	Gefährdungspotentiale von Funknetzen	168
6.1.1	Physikalische Aspekte	168
6.1.2	Netzwerktechnik	169
6.1.3	Übertragungstechnik	170
6.1.4	Betriebliche Aspekte	172
6.2	Sicherheit nach IEEE 802.11	173
6.2.1	WEP	173

6.2.2	Authentisierung	181
6.2.3	Verbindungsaufbau im WLAN	185
6.2.4	Angriffsszenarien	188
6.2.5	Tools	201
6.3	Ein erweiterter Anforderungskatalog	203
6.4	Die neuen Kryptografieverfahren	207
6.4.1	CCMP	207
6.4.2	TKIP	213
6.4.3	WPA	217
6.4.4	Vergleich der Frameformate	218
6.5	Authentisierung	219
6.5.1	IEEE 802.1X	219
6.5.2	802.1X-Integration in WLANs	226
6.5.3	Pre-Shared Keys	227
6.6	Schlüsselverwaltung	228
6.7	Robust Security Network	234
6.7.1	Scanning	237
6.7.2	Roaming	238
6.7.3	Sicherheitsklassen und Migration	241
6.8	Zusammenfassung des Frame-Austauschs	246
6.9	Fazit und Ausblick	250

## **7    **PRODUKTE**    **252****

7.1	Marktsituation - Marktentwicklung	252
7.2	Ausstattung	254
7.3	Die Tests	262
7.4	Durchsatz und Reichweite	265
7.4.1	Ausleuchtung in der Fläche	269
7.4.2	Short-Header-Format und Long-Header-Format	273
7.4.3	Migration von 802.11b nach 802.11a	275
7.5	Kanalinterferenz im 2,4-GHz-Band	277
7.6	Overhead des RTS/CTS-Verfahren	279

7.7	Thin Access Points	280
<b>8</b>	<b><u>MESSTECHNIK FÜR WIRELESS LAN</u></b>	<b>281</b>
8.1	Spektrumanalysator	281
8.2	Client-Utilities	286
8.3	Spektrumanalysator vs. Client Utility	291
8.3.1	Testaufbau (Outdoor)	291
8.3.2	Ergebnisse	292
8.4	Protokollanalyatoren	296
<b>9</b>	<b><u>EINSATZ EXTERNER ANTENNEN</u></b>	<b>299</b>
9.1	Testaufbau	299
9.2	Messergebnisse	301
9.2.1	AIR-ANT 5959 von Cisco bzw. S2402DS24MMX von Cushcraft	301
9.2.2	SPA 2400/360/4/20/V von Huber & Suhner	305
9.2.3	PCW24-07008-AML von SmartAnt	307
9.2.4	EMW24-03005-AML von SmartAnt	310
9.2.5	Integrierte Antenne im Enterasys Client-Adapter	312
9.3	Koaxialverbinder	314
9.4	Kabeltypen	317
9.5	Pigtails	318
9.6	Konsequenzen	319
<b>10</b>	<b><u>AUFBAU VON WIRELESS LANS</u></b>	<b>321</b>
10.1	Konzepte	321
10.1.1	LAN-Erweiterung	321
10.1.2	LAN-Erweiterung in unterschiedliche IP-Subnetze	322
10.1.3	Sicherheit über IPSec-Tunnel	325
10.1.4	Überdeckung einer großen Fläche	326
10.1.5	Viele Clients auf beschränktem Raum	328
10.1.6	Ausfallsicherheit	329

10.1.7	Vergrößerung einer bestehenden Funkzelle	330
10.1.8	Funkverbindung zweier Ethernet-LANs	331
10.2	Strukturierte Funknetze	332
10.2.1	Die Rolle des Distribution System	332
10.2.2	Distribution System hinter einer Firewall	337
10.2.3	Distribution System als VPN	339
10.2.4	Die Rolle des Clients	341
10.2.5	Öffentliche WLANs	344
10.3	Planung	345
10.3.1	Konzeptphase	345
10.3.2	Zellplanung	347
10.3.3	Planung der passiven Komponenten des Distribution System	357
10.3.4	Planung der aktiven Komponenten des Distribution System	358
10.3.5	Planung der WLAN-Sicherheitsinfrastruktur	358
10.4	Wireless oder Kabel: Ein beispielhafter Kostenvergleich	360
10.4.1	Passive Komponenten	360
10.4.2	Aktive Netztechnik	365
10.4.3	Gesamtkosten im Vergleich	372
<b>11</b>	<b><u>WEITERE ASPEKTE - NEUE ENTWICKLUNGEN</u></b>	<b>373</b>
11.1	Rechtliche und gesundheitliche Aspekte	373
11.2	Windows XP	376
<b>12</b>	<b><u>AUF DEM WEG ZUM KABELLOSEN ACCESS?</u></b>	<b>378</b>
12.1	Fazit	380
	<b><u>ANHANG</u></b>	<b>383</b>
A	Tabellen zum FHSS-Verfahren	383
A.1	Kanäle und Frequenzen beim FHSS	383
A.2	Sprungfolgen beim FHSS	383
A.3	Hopping Sets beim FHSS	384

B	Tabellen zum DSSS-Verfahren	385
B.1	Kanäle und Frequenzen beim DSSS	385
B.2	Hopping Sets beim DSSS	385
C	Auszug aus dem ERC Report 25	386
D	Frametypen	389
E	Konstruktion eines gültigen CRC für gefälschte Frames	390
F	Detailprotokolle von Frame-Abfolgen	391
F.1	Anmeldung an einem „Open System“	391
F.2	Anmeldung an einem „Closed System“	400
<b><u>ABBILDUNGSVERZEICHNIS</u></b>		<b><u>411</u></b>
<b><u>TABELLENVERZEICHNIS</u></b>		<b><u>420</u></b>
<b><u>INDEX</u></b>		<b><u>422</u></b>
<b><u>ABKÜRZUNGEN</u></b>		<b><u>429</u></b>
<b><u>LITERATUR</u></b>		<b><u>436</u></b>