Achtung! Siemens WLAN!

KOEXISTENZ VON „ STANDARD“ WLAN UND SIEMENS I-WLAN

- Der erste WLAN (BreezeACCESS, FHSS, 3 Mb/s): 2001
- Der erste nicht Wi-Fi Wireless Netzwerk (WALKair, PDH/SDH): 2004
- Das größte Cisco WLAN : 60 Lokationen, 950 APs
- Das größte ExtremeWiNG WLAN: 1100 Lokationen, 4000 APs
- Der erste Cloud WLAN Projekt: XIQ, 15 Lokationen, 150 APs

- Zertifikate von: Ruckus, Comscope, Cisco, Extreme Wireless, Siemens
- CWNE#487

Twitter: @ITunakin

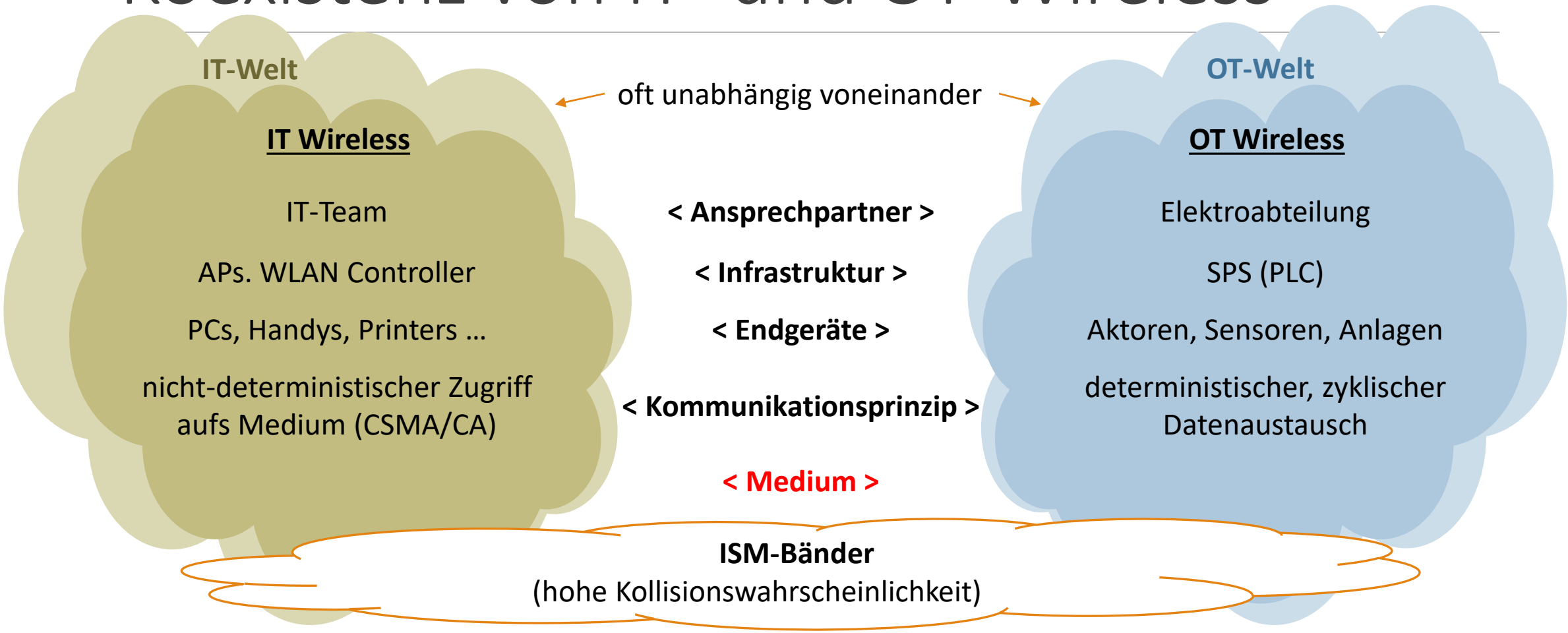
Blog: www.mywlannotes.blogspot.com

Email: igor@tunakin.de

Agenda

- Problemstellung: IT und OT Koexistenz
- Wiederholung: 802.11 PCF Modus
- Vergleich PCF und DCF
- Siemens iPCF vs. 802.11 PCF
- Praktischer Teil

Koexistenz von IT- und OT-Wireless



802.11 standard Zugriffsverfahren

	contention based (CSMA/CA)	**contention free (Deterministisch)**
Non QoS	Distributed Coordination Function (**DCF**) • Carrier sense / Listen-Before-Talk • Random backoff timer (contention window) • Interframe spaces (RIFS, SIFS, DIFS, AIFS, EIFS) • Duration/ID field • RTS/CTS	Point Coordination Function (**PCF**) • AP is the Point Coordinator (PC) • two periods between Beacons: CFP and CP • PCF interframe spacing (PIFS) < DIFS, AIFS • Poll based access to the medium
QoS	Enhanced Distributed Channel Access (**EDCA**) New interframe spaces: • AC_BK (Background), • AC_BE (Best Effort), • AC_VI (Video), • AC_VO (Voice)	HCF Controlled Channel Access (**HCCA**) • AP is the Hybrid Coordinator (HC) • Controlled Access Phase (CAP) (Beacons independent) • Traffic Class (TC) and Traffic Streams (TS) for QoS • stations are given a TXOP

Koexistenz PCF & DCF

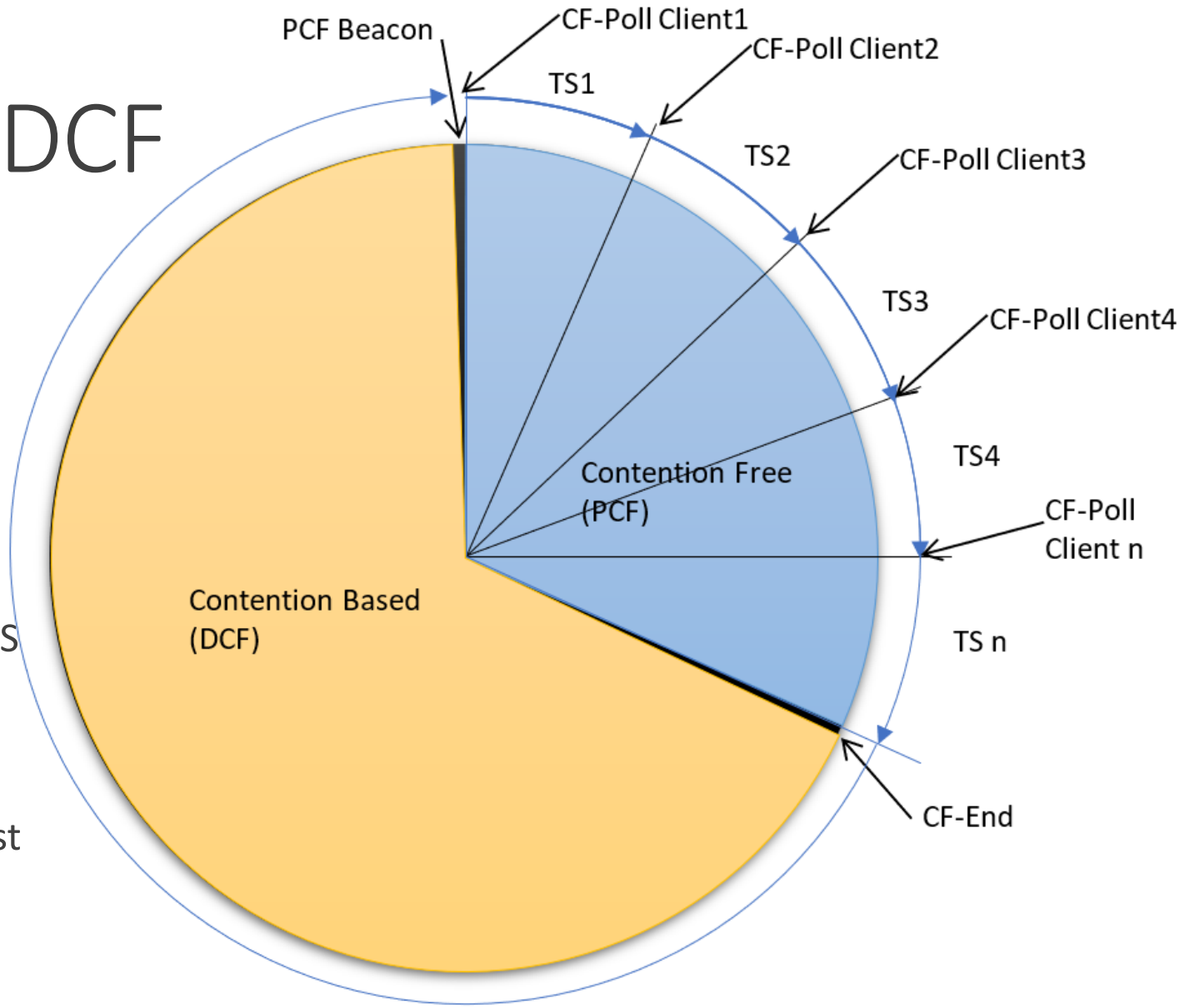
1. Der PCF-AP wartet während PIFS und versendet den Beacon, in dem zwei Zeiträume definiert werden:
   - Contention Free (or PCF) (startet direkt nach dem Beacon)
   - Contention Based (CSMA/CA)

2. Der AP sendet CF-Poll Packet an jeden Client nacheinander.

Der Intervall zwischen PCF-Paketen ist SIFS oder PIFS

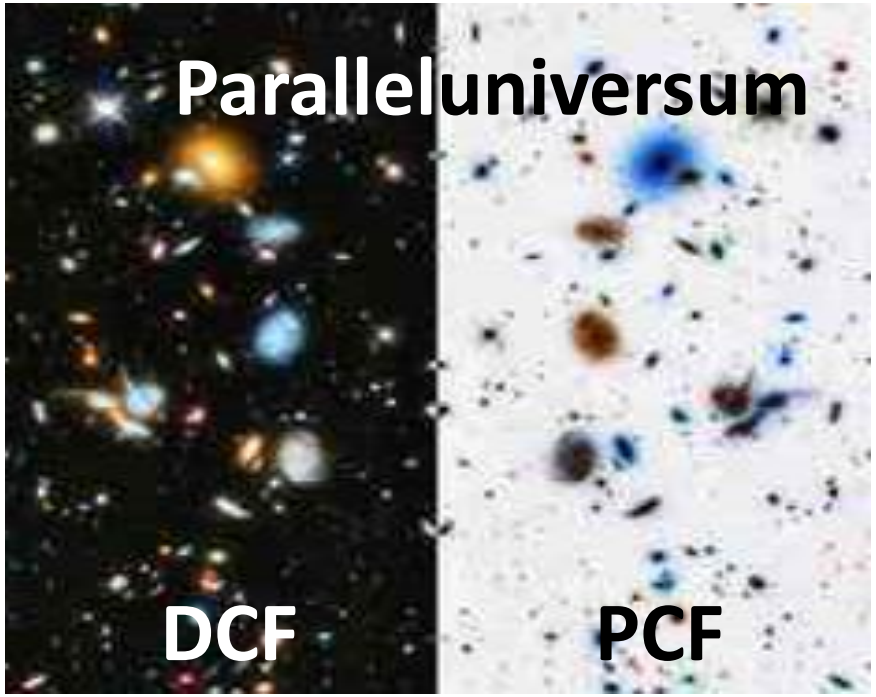
SIFS	**<** 9µs	**PIFS** (SIFS + 1*Slot)	**<** 9µs	**DIFS** (SIFS + 2*Slot)

➔ Selbst wenn ein DCF-STA den PCF-Beacon verpasst hat, hat er keine Chance, das Senden zu starten, da der Backoff-Zähler nicht weiter zählt solange SIFS zwischen Paketen ist.



Vergleich PCF und DCF

		DCF	PCF
	Kollisions-vermeidung	CSMA/CA	zentrale Steuerung
Echtzeit-kommunikation	**Overhead**	Mehr (Backoff, RTS/CTS..)	weniger
	Kommunikation	Nicht-deterministisch	Deterministisch
	Jitter	mehr	weniger
	Priorität	niedriger	höher
	Skalierbarkeit	Nicht-deterministisch	Deterministisch
	Störfestigkeit	mehr	weniger
	Datendurchsatz	mehr	weniger



Quelle: Wissenschaftler sehen Hinweise auf ein umgekehrtes Paralleluniversum (forschung-und-wissen.de)

CWNA official Study Guide, 4th Edition, page 272: *„As we stared earlier, PCF is an **optional** access method, and as of this writing, **we do not know of any vendor that has implemented it**.“*

iPCF von Siemens

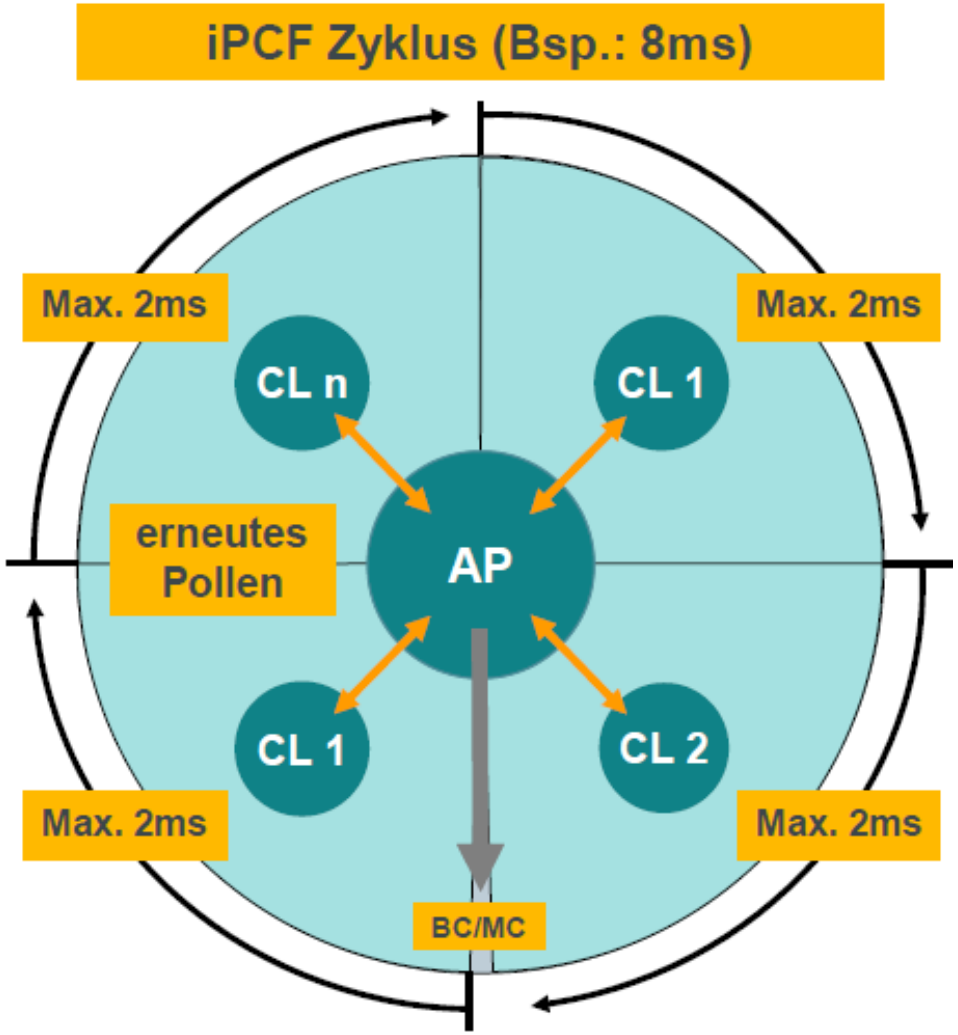
- **iWLAN** (Industrial W-LAN) von Siemens ist ein komplettes Eko-System (eigene APs, Clients, L2, L3, L4 Protokolle, SW)

- **iPCF** und **iPCF-MC** sind proprietäre Protokolle für **MAC**-Ebene (Layer 2) im iWLAN

- Für die PHY-Ebene verwendet Siemens iWLAN OFDM(11.a), HT(11.n) und HE(11.ax) in der Zukunft in Rahmen iPCF-2

Feste Zykluszeiten 8 / 16 / 32 / 64 / 128 / 256 / 512 ms

Jeder Client hat ein Zeitfenster von maximum 2 ms zur Verfügung.

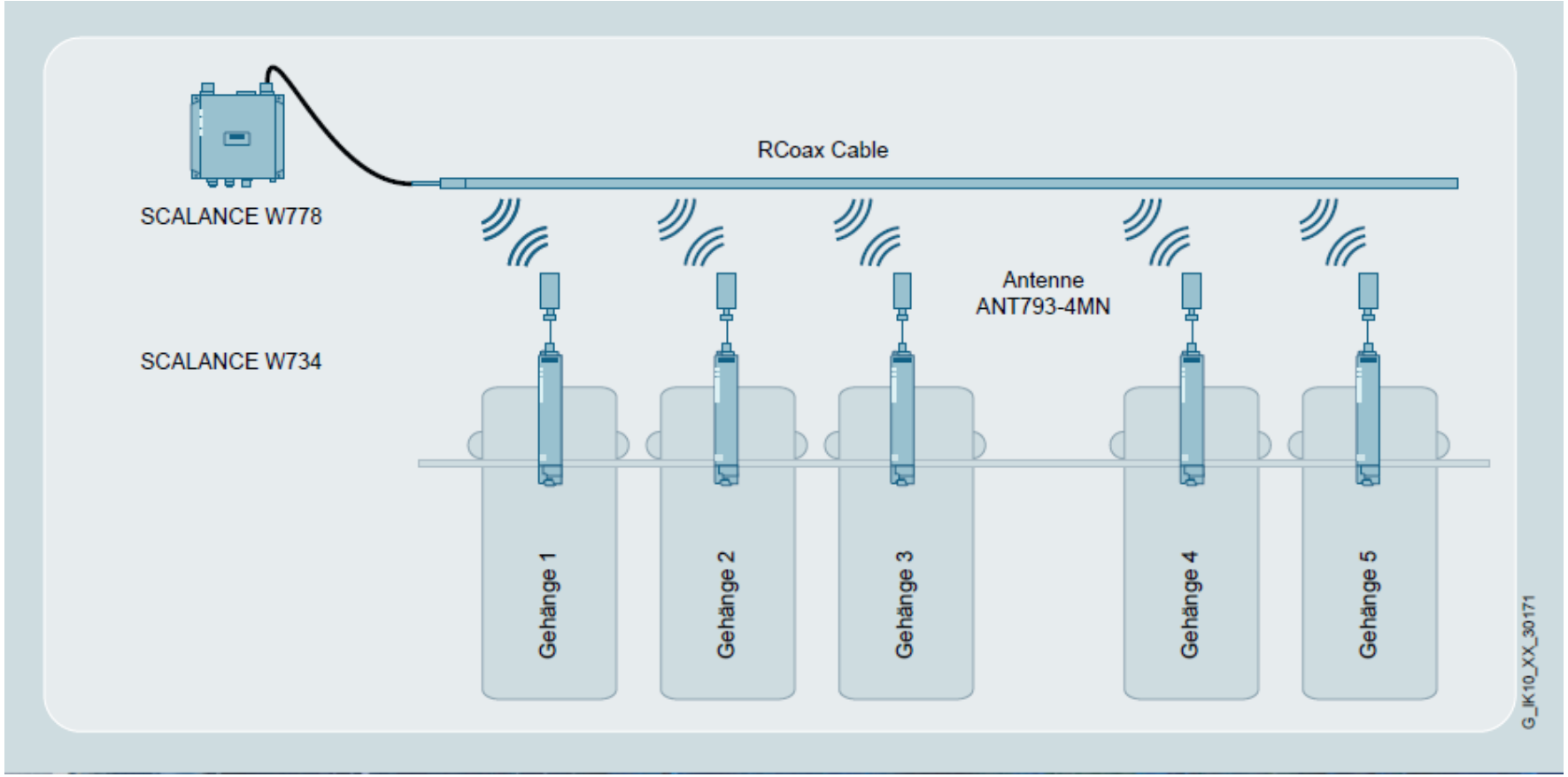


iPCF - Modus

Merkmale
- Einsatz des RCoax-Leckwellenleiters

Roaming
- Client scannt, wenn er die Verbindung zum AP verliert

Anwendungen
- Fertigungslinien
- automatische Lagersysteme
- Einschienenhängebahnen



Quelle: iFeatures – industrielle Zusatzfunktionen für drahtlose Anwendungen | Ausgabe 09/2017

iPCF-MC - Modus

Merkmale

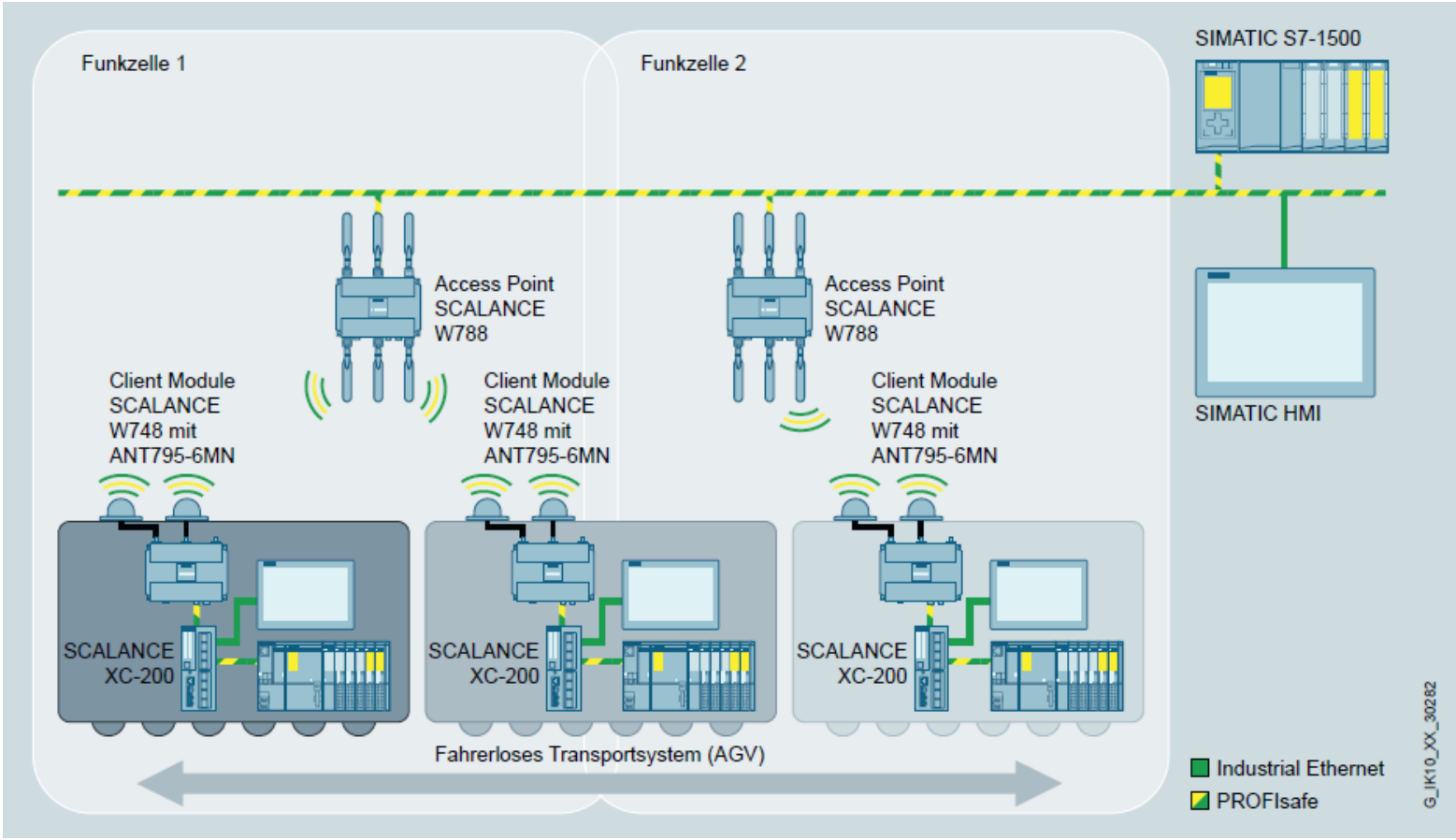
- Jeder AP nutzt zwei Funkschnittstellen (zwei Kanäle) gleichzeitig (ein Kanal für Daten und ein Kanal für Mgmt)
- Alle APs haben gleichen Mgmt-Kanal konfiguriert.

Roaming

- Client scannt den Management-Kanal (MC) bevor er roamt.

Anwendungen:

- fahrerlosen Transportsystemen (AGV)
- Krananwendungen



Quelle: iFeatures – industrielle Zusatzfunktionen für drahtlose Anwendungen | Ausgabe 09/2017

Siemens iPCF vs. 802.11 PCF (1)

	PCF	iPCF-MC	iPCF
Erste Anmeldung	Wie bei DCF (mehr Overhead)	2 Frames (~5ms)	
Anzahl der Zyklen pro Beacon	1 pro Beacon-Periode	Unabhängig von Beacon-Periode	
PCF-Zyklusdauer	Flexibel	Fest: 8 / 16 / … / 512 ms	
Zeit per Client	N/A	2 ms	
Max. Client per AP	N/A	256	
Roaming-Trigger	Beacon-Verlust, Signalpegel, Packet-Verlust (wie bei DCF)		kein Empfang vom AP
Verschlüsselung	wie beim DCF	AES128 + proprietäres Protokoll (nur iPCF-Geräte haben Zugriff)	
Kompatibilität mit Automatisierungsprotokollen wie PROFINET	nein	ja	
Koexistenz mit DCF	Ja, höhere Priorität	**Nein, Konkurrenz**	

Siemens iPCF vs. 802.11 PCF (2)

Typ	**PCF** Sub-Typs		**iPCF** Sub-Typs
00 Mgmt	0000 Association Request 0001 Association response 0010 Reassociation Request 0011 Reassociation Response 0100 Probe Request	0101 Probe Response 1000 Beacon 1010 Disassociation 1011 Authentication 1100 Deauthentication	1000 Beacon
01 Control	1101 ACK	1110 CF-End 1111 CF-End+CF-Ack	1101 ACK
10 Data	0001 Data+CF-Ack 0010 Data+CF-Poll 0011 Data+CF-Ack+CF-Poll	0101 CF-Ack(No Data) 0110 CF-Poll(No Data) 0111 CF-Ack+CF-Poll(No Data)	
11 Extention			0010 S1G Beacon 0011 Pull/Data 1000 Association Request 1001 Association Response

Indikatoren der iPCF Kommunikation

1 Beacon pro Sekunde

No.	D.Time	Transmitter address	Receiver address	Frame Type	Type	Subtype	Data rate	MCS
16	1.024000	20:87:56:35:f6:d8	ff:ff:ff:ff:ff:ff	Beacon	Management frame	8	12	
17	1.024000	20:87:56:35:f6:d8	ff:ff:ff:ff:ff:ff	Beacon	Management frame	8	12	
18	1.024000	20:87:56:35:f6:d8	ff:ff:ff:ff:ff:ff	Beacon	Management frame	8	12	
19	1.024000	20:87:56:35:f6:d8	ff:ff:ff:ff:ff:ff	Beacon	Management frame	8	12	
20	1.024000	20:87:56:35:f6:d8	ff:ff:ff:ff:ff:ff	Beacon	Management frame	8	12	
21	0.627000		20:87:56:35:f6:d8		Extension frame	8	6	
22	0.000000		00:1b:1b:92:c8:68	Ack	Control frame	13	6	
23	0.000000		00:1b:1b:92:c8:68		Extension frame	9	19,5	2
24	0.000000		20:87:56:35:f6:d8	Ack	Control frame	13	6	
25	0.001000		00:1b:1b:92:c8:68		Extension frame	2	19,5	2
26	0.002000		20:87:56:35:f6:d8	Ack	Control frame	13	6	
27	0.000000		20:87:56:35:f6:d8		Extension frame	2	19,5	2
28	0.000000		00:1b:1b:92:c8:68	Ack	Control frame	13	6	
29	0.002000		00:1b:1b:92:c8:68		Extension frame	2	19,5	2
30	0.000000		20:87:56:35:f6:d8	Ack	Control frame	13	6	
31	0.000000		20:87:56:35:f6:d8		Extension frame	2	19,5	2
32	0.000000		00:1b:1b:92:c8:68	Ack	Control frame	13	6	
33	0.003000		00:1b:1b:92:c8:68		Extension frame	2	19,5	2

MCS 2 für alle Extension Frames

Nur eine MAC-Adresse

Frames von Extension-Typ (wlan.fc.type == 3) und Sub-Typ 2,8, und 9

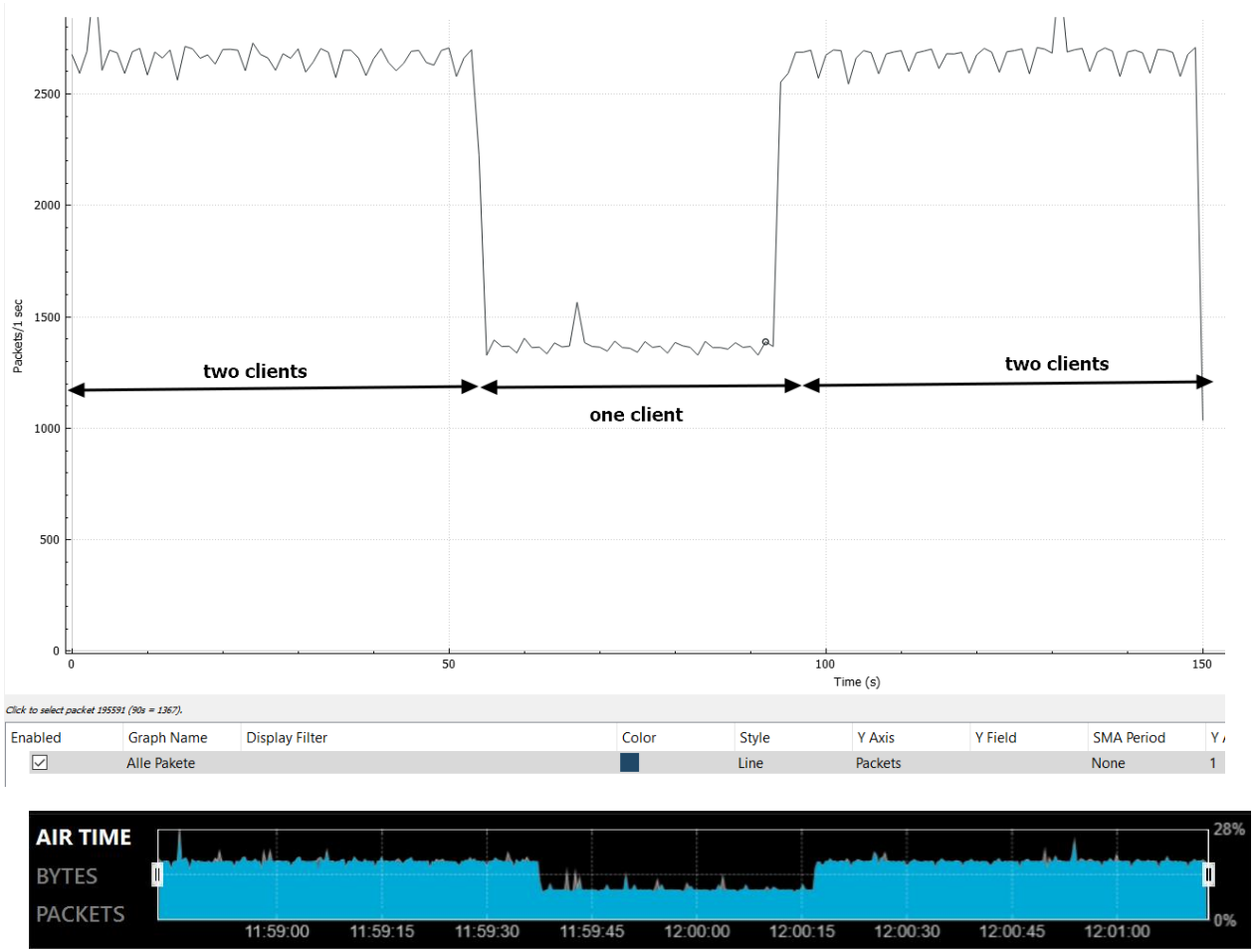
iPCF Kommunikation | Airtime

No.	D.Time	Comment	Receiver address	Frame Type
14	0.000006	AP --> Client 1	00:1b:1b:de:6c:b8	Pool/Data
15	0.000004		00:1b:1b:f0:ba:a8	Ack
16	0.000006	Client 1	00:1b:1b:f0:ba:a8	Pool/Data
17	0.000008		00:1b:1b:de:6c:b8	Ack
18	0.002818	AP --> Client 1	00:1b:1b:de:6c:b8	Pool/Data
19	0.000143		00:1b:1b:f0:ba:a8	Ack
20	0.000010	Client 1	00:1b:1b:f0:ba:a8	Pool/Data
21	0.000007		00:1b:1b:de:6c:b8	Ack
22	0.000006	AP -- Client 2	00:1b:1b:de:6c:88	Pool/Data
23	0.000006		00:1b:1b:f0:ba:a8	Ack
24	0.000006	Client 2	00:1b:1b:f0:ba:a8	Pool/Data
25	0.000009		00:1b:1b:de:6c:88	Ack
26	0.002866	AP --> Client 2	00:1b:1b:de:6c:88	Pool/Data
27	0.000018		00:1b:1b:f0:ba:a8	Ack
28	0.000005	Client 2	00:1b:1b:f0:ba:a8	Pool/Data
29	0.000006		00:1b:1b:de:6c:88	Ack
30	0.000006	AP -- Client 1	00:1b:1b:de:6c:b8	Pool/Data
31	0.000005		00:1b:1b:f0:ba:a8	Ack
32	0.000005	Client 1	00:1b:1b:f0:ba:a8	Pool/Data
33	0.000007		00:1b:1b:de:6c:b8	Ack
34	0.002791	AP --> Client 1	00:1b:1b:de:6c:b8	Pool/Data
35	0.000017		00:1b:1b:f0:ba:a8	Ack
36	0.000005	Client 1	00:1b:1b:f0:ba:a8	Pool/Data
37	0.000006		00:1b:1b:de:6c:b8	Ack

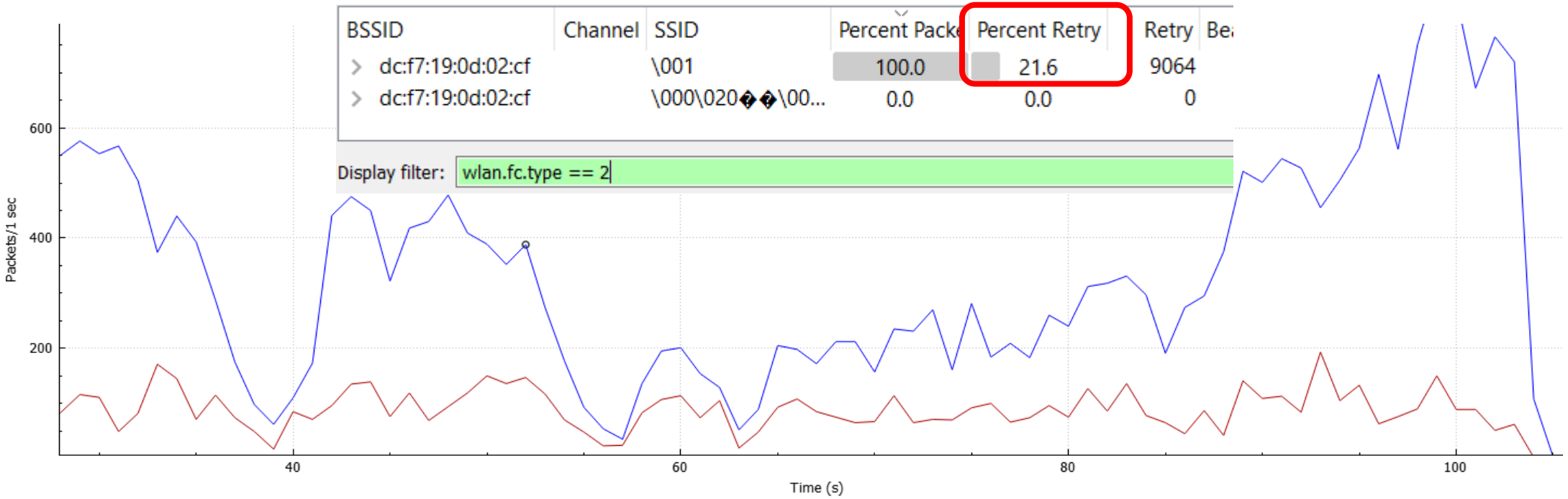
TS1

TS2

TS3



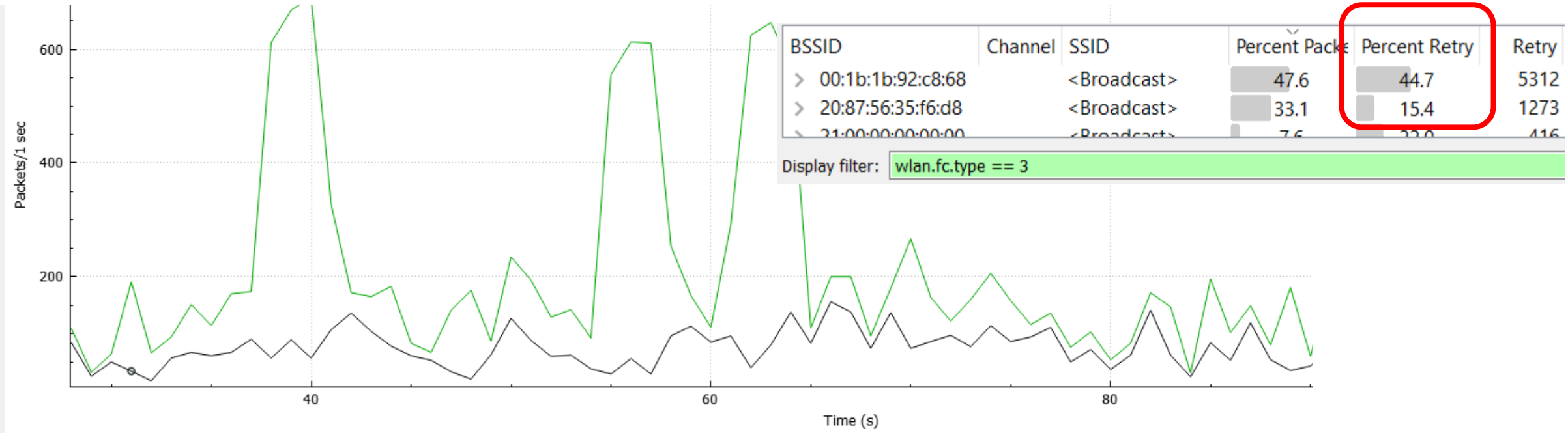
Koexistenz von iPCF & DCF (aus DCF Sicht)



lick to select packet 77291 (52s = 388).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	DCF Data	wlan.fc.type == 2		Line	Packets		None	1
☑	DCF Data Retry	wlan.fc.type == 2 && wlan.fc.retry == 1		Line	Packets		None	1
☐	iPCF Data	wlan.fc.type == 3		Line	Packets		None	1
☐	iPCF Data Retry	wlan.fc.type == 3 && wlan.fc.retry == 1		Line	Packets		None	1

Koexistenz von iPCF & DCF (aus iPCF Sicht)



Click to select packet 52484 (31s = 34).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☐	DCF Data	wlan.fc.type == 2		Line	Packets		None
☐	DCF Data Retry	wlan.fc.type == 2 && wlan.fc.retry == 1		Line	Packets		None
☑	iPCF Data	wlan.fc.type == 3		Line	Packets		None
☑	iPCF Data Retry	wlan.fc.type == 3 && wlan.fc.retry == 1		Line	Packets		None

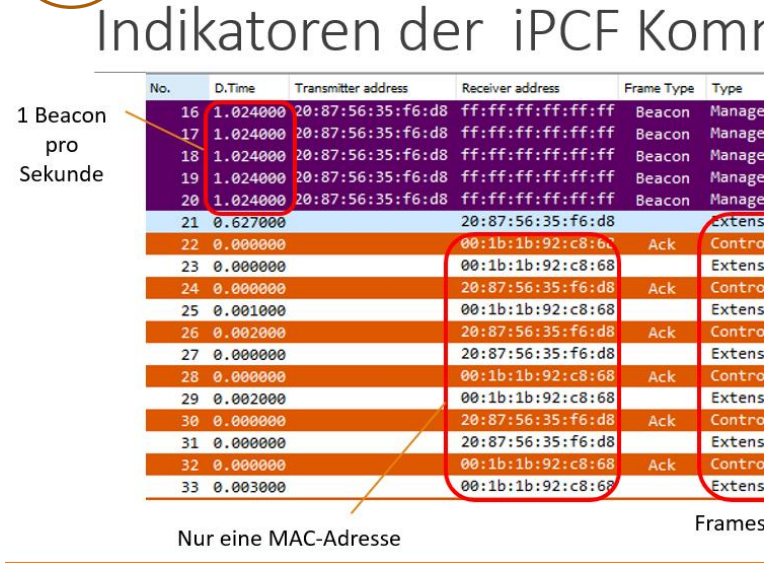
Empfehlungen

1 **wenden an Elektroabteilung**

Quelle: https://verdi-drupa.de/2017/02/06/print-4-0/

2 **WLAN scannen**

3 **WLAN sniffen**



Falls ein **iPCF** WLAN entdeckt wurde:

- **Gleiche Kanäle sind verboten!**
- **dem Auftraggeber die Frequenz-Planug empfehlen**

Zusammenfassung

$iPCF \in \{Siemens\ iWLAN\}$

$iPCF \neq PCF$

$iPCF\text{-}MC = \{MC, DC\}$

$MC_{AP1} = MC_{AP2} = .. = MC_{APn}$

$Data\ Rate_{DC} = MCS\ 2$

$\boldsymbol{(iPCF + DCF)_{Kanal\ N} = 0}$


Danke