HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

INSTITUTE FOR INTERNET
TECHNOLOGIES AND APPLICATIONS

Aufbau und Entwicklung einer WLAN-Messumgebung zur Untersuchung des QoS des G- und N- Standards

Studienarbeit

Abteilung Informatik

Hochschule für Technik Rapperswil

Frühjahrssemester 2012

Autor: Fabian Beck

Betreuer: Prof. Dr. Rinkel Andreas

INHALT

AUFGABENSTELLUNG

Das Ziel dieser Arbeit ist es, einen systematischen Ansatz zum Aufbau und zur Realisierung einer WLAN-Messumgebung des G-und N-Standards zu erarbeiten und umzusetzen. Dazu sind erst die Grundlagen von WLANs zu erarbeiten, zu dokumentieren und hinsichtlich der Messwerterfassung zu bewerten. Ferner sollen mit der entwickelten Messumgebung Referenzmessungen erstellt werden, um Systeme im Feld besser bewerten zu können. Dies beinhaltet sowohl die Erarbeitung eines Mess-Setups als auch die Entwicklung verschiedener Messszenarien, welche dann in der Praxis umgesetzt und ausgewertet werden können. Die Messszenarien sollen die Antworten auf folgende Fragestellungen beinhalten:

- Was soll gemessen werden?
- Wie wird gemessen?
- Was sind die zu erwartenden Ergebnisse?

Nach der Erarbeitung der Mess-Setups und der Szenarien sollen die Messungen auf zwei Arten durchgeführt werden. Erstens in einem gestörten WLAN-Umfeld und zweitens in einem ungestörten Umfeld. Dazu kann die HF-Kammer an der Hochschule für Technik in Rapperswil benutzt werden. Die Resultate sind dann auszuwerten, zu interpretieren und zu vergleichen.

Rapperswil, 29.05.2012

Andreas Rinkel

EIGENSTÄNDIGKEIT DER ARBEIT

Erklärung

Ich erkläre hiermit,

- dass ich die vorliegende Arbeit selber und ohne fremde Hilfe durchgeführt habe, ausser derjenigen, welche explizit in der Aufgabenstellung erwähnt ist oder mit dem Betreuer schriftlich vereinbart wurde,
- dass ich sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt angegeben habe.

Rapperswil, 01.06.2012:

Fabian Beck

ABSTRACT

In dieser Arbeit wird eine WLAN-Messumgebung entwickelt und aufgebaut, um die Geschwindigkeiten von WLANs im G- und N-Standard zu analysieren.

Basierend auf einer Analyse der Standards werden die Messszenarien unter Berücksichtigung des Physical- und MAC-Layer definiert. Insbesondere wird der Einfluss der unterschiedlichen Protokollmechanismen auf Durchsatz, Jitter und Paket-Loss untersucht. Zu den Protokollmechanismen im G-Standard gehören unter anderem die Short/Long Preamble, der RTS/CTS Mechanismus und die verschiedenen QoS-Klassen. Die Messszenarien für den N-Standard beinhalten das Short/Long Guard Intervall, die Frame Aggregation als auch die Verwendung von RIFS.

Nach dem Aufbau und der Entwicklung der Messumgebung werden die verschiedenen Messszenarien, in einem gestörten Umfeld und in einer HF-Kammer durchgeführt. Dabei wird sichtbar, was Störeinflüsse für einen Einfluss auf den Durchsatz, Jitter und den Packet-Loss von WLANs haben.

Diese Arbeit führt zum Ergebnis, dass nun Referenzmessungen vorhanden sind, mit denen WLANs im Feld besser analysiert werden können und mit denen eine Aussage gemacht werden kann, welche Protokollmechanismen aktiviert werden müssen, um den Durchsatz von WLANs zu erhöhen.

MANAGEMENT SUMMARY

Die Geschwindigkeit von WLANs ist aufgrund der Fremdstörungen schwierig genau zu messen. Die bis her publizierten Messungen zu WLANs sind aus diesem Grund nicht eindeutig reproduzierbar und liefern daher nur eingeschränkte Aussagen über die erreichbaren Datenrate unter bestimmt Rahmenbedingungen.

Aus diesem Grund wird in dieser Arbeit zwischen einer störungsfreien Testumgebung (HF-Kammer) und einer gestörten Testumgebung unterschieden. Dazu werden die verwendeten Geräte wie Notebooks, Access Point und deren Protokollmechanismen genau analysiert und beschrieben. Des Weiteren werden auch die Umgebungen, in der die Messungen ausgeführt werden, beschrieben und bewertet. Durch die Messszenarien ist genau ersichtlich, welche Protokollaspekte des Kommunikationsstacks in der Messung berücksichtigt werden. Die gleichen Messszenarien werden in einem gestörten und in einem ungestörten Umfeld durchgeführt.

Dank der vergleichenden Auswertung der Messszenarien ist es nun einerseits ersichtlich, welche Protokollmechanismen aktiviert/deaktiviert werden müssen, um den Durchsatz von WLANs zu erhöhen. Andererseits können die vergleichenden Messungen auch als Referenzmessungen genutzt werden, um Übertragungs- oder Leistungsprobleme im Feld besser analysieren zu können.

AUFBAU DER ARBEIT

Im Kapitel Grundlagen wird der theoretische Hintergrund zu WLANs vermittelt. Des Weiteren werden die für diese Arbeit relevanten Standards und Protokolle beschrieben. Dazu gehören der G-, E- und N-Standard sowie verschiedene Kontroll- und Management-Protokolle, welche in diesen Standards verwendet werden.

Im Kapitel Mess-Hardware werden die Produkte vorgestellt, welche für die Messungen verwendet wurden. Dabei umfasst die Beschreibung der Hardware nur jene Funktionen, die für diese Arbeit relevant sind.

Das Kapitel Mess-Software gibt eine Einführung in das Programm, welches für die Messungen verwendet wurde. Dabei werden die Funktionen und Einstellungsmöglichkeiten des Programms erläutert.

Das Kapitel Messaufbau erläutert die Infrastruktur, welche für die Messungen verwendet wurde. Des Weiteren werden die Netzwerkprotokolle, welche bei der Messung verwendet wurden, mittels TCP/IP-Referenzmodell dargestellt und beschrieben. Zusätzlich wird in diesem Kapitel auch auf Probleme eingegangen, welche die Messungen beeinflussen, wie beispielsweise die Round Trip Time oder die Synchronisation von Uhren.

Im Kapitel Messszenarien werden verschiedene Szenarien dargestellt, in denen die Performance von WLANs gemessen wird. Es werden Referenzmessungen zu den verschiedenen implementierten Technologien/Funktionen durchgeführt, welche in den WLAN-Standards 802.11g, 802.11e und 802.11n eingesetzt werden.

Das Kapitel Messumgebung beschreibt die beiden Umgebungen, in denen die Messungen für diese Arbeit durchgeführt wurden.

Im Kapitel Messauswertung sind alle durchgeführten Messungen mit Diagrammen aufgeführt. Sie beinhalten die Round Trip Time mit ICMP und TCP, die Verarbeitungszeit der verwendeten Access Points und die Auswertung der verschiedenen Protokollmechanismen der Standards.

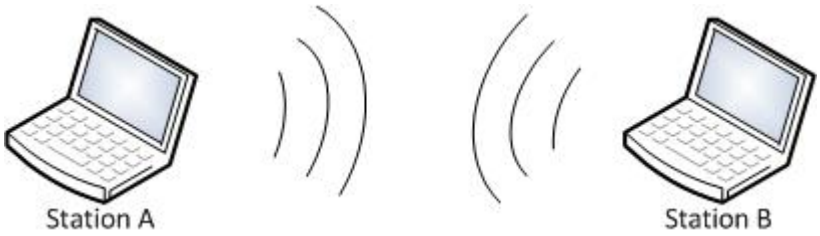
GRUNDLAGEN

WLAN-MODI

WLANs werden vom Aufbau her in zwei verschiedene Kategorien unterteilt.

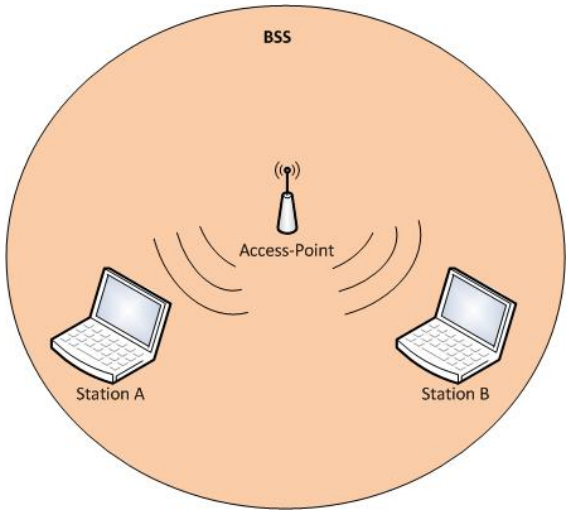
AD-HOC-MODUS

Der Ad-hoc-Modus ist ein Betriebsmodus, in dem die einzelnen Stationen über ihre integrierte WLAN-Netzwerkkarte untereinander kommunizieren. Die Kommunikation findet direkt zwischen den einzelnen Stationen statt. Somit ist es möglich, ein Peer-to-Peer-Netzwerk über Funk zu betreiben. Dieser Modus wird im Fachjargon auch als IBSS (Independent Basic Service Set) bezeichnet.



INFRASTRUKTUR-MODUS

Der Infrastruktur-Modus ähnelt sehr einem geswitchten Netzwerk. Es gibt eine zentrale Stelle, mit der die verschiedenen Stationen über die Luft verbunden sind. Diese Stelle heisst Access Point. Die Kommunikation zwischen den Stationen findet immer über den Access Point statt. Dieser Modus wird als BSS (Basic Service Set) bezeichnet. Solange die Station in der Reichweite des Access Point ist, bleibt sie mit ihm verbunden. Deshalb ist man bei diesem Modus sehr mobil. Zur weiteren Ausdehnung des Funknetzwerks kann man mehrere BSS zu einem ESS (Extended Service Set) zusammenfassen. Jeder Access Point bildet dabei eine Funkzelle. Wenn eine Station bemerkt, dass die Sendeleistung der Funkzelle abnimmt, aber gleichzeitig über eine andere Funkzelle ein stärkeres Signal empfängt, dann kann sie sich mit dem Access Point dieser Funkzelle verbinden. Dieser Vorgang wird als Roaming bezeichnet. Somit erreicht man eine sehr hohe Funkabdeckung und die Benutzer können sich im Raum frei bewegen, ohne dass sie die Verbindung zum WLAN verlieren – vorausgesetzt, sie bleiben in Reichweite des Access Point.



FREQUENZBAND

Da WLANs Daten über das Medium Luft versenden, müssen zur Übertragung der Daten Frequenzbänder verwendet werden. Für WLANs wurden zwei Frequenzbereiche im ISM-Band festgelegt. Der Vorteil des ISM-Bandes ist, dass es weltweit lizenz- und genehmigungsfrei für industrielle, medizinische und wissenschaftliche Anwendungen genutzt werden darf. Das eine Frequenzband ist im 2.4-GHz- und das andere im 5-GHz-Bereich. Diese Frequenzbänder werden in sogenannte Kanäle unterteilt, welche für die Übertragung von Daten verwendet werden können.

2.4-GHZ-BEREICH

Im 2.4-GHz-Bereich sind in Europa 13 verschiedene Kanäle vorhanden. Ein Kanal besitzt eine Bandbreite von 22 MHz. Der Abstand zwischen den einzelnen Kanälen ist 5 MHz breit. Das bedeutet, dass es innerhalb des 2.4-GHz-Bereichs lediglich drei verschiedene Kanäle gibt, die sich nicht überlappen, nämlich Kanal 1, 7 und 13. Bei der Planung von WLANs muss man daher darauf achten, dass man einen Kanal wählt, der sich nicht mit anderen Kanälen überlappt. Ansonsten läuft man Gefahr, dass sich die WLANs gegenseitig stören. Eine solche Störung wirkt sich negativ auf die Performance aus und es würde zwangsläufig zu Kollisionen kommen. Die Sendeleistung in diesem Bereich ist auf maximal 100 mW beschränkt.

Ein weiteres Problem dieses Bandes ist, dass es auch von anderen Technologien verwendet wird. Hierzu gehören Bluetooth, Mikrowellenherde, Funkkameras etc. Die Verwendung dieser Geräte hat einen negativen Einfluss auf die Performance des WLAN.

Kanalnummer	Trägerfrequenz (GHz)	Frequenzbereich (GHz)
1	2.412	2.401 – 2.423
2	2.417	2.406 – 2.428
3	2.422	2.411 – 2.433
4	2.427	2.416 – 2.438
5	2.432	2.421 – 2.443
6	2.437	2.426 – 2.448
7	2.442	2.431 – 2.453
8	2.447	2.436 – 2.458
9	2.452	2.441 – 2.463
10	2.457	2.446 – 2.468
11	2.462	2.451 – 2.473
12	2.467	2.456 – 2.478
13	2.472	2.461 – 2.483

5-GHZ-BEREICH

Im Jahre 2002 wurde in Europa ein weiteres Frequenzband für die Benutzung von WLANs freigegeben. Allerdings wird wie der 2.4-GHz-Bereich auch dieser Frequenzbereich von anderen Diensten mitbenutzt. Beispiele dafür sind militärische Radarsysteme, Satelliten- und Amateurfunk.

Das 5-GHz-Band ist in drei Unterbänder aufgeteilt. Die ersten beiden Unterbänder sind im Bereich von 5.15–5.25 GHz bzw. von 5.25–5.35 GHz. Jedes dieser Unterbänder besitzt vier Kanäle. Jeder Kanal besitzt eine Bandbreite von 20 MHz. Auf diesen zwei Unterbändern ist eine Sendeleistung von maximal 200 mW erlaubt. Aufgrund der Tatsache, dass das 5-GHz-Band auch von anderen Diensten benutzt wird, muss sichergestellt werden, dass man keine Kanäle von solchen Einrichtungen benutzt. Um das zu erreichen, muss DFS (Dynamic Frequency Selection) unterstützt werden. DFS stellt einen automatischen Frequenzwechsel sicher, falls ein Kanal bereits von einem anderen Dienst benutzt wird. Ist DFS nicht implementiert, so darf nur der Frequenzbereich von 5.15–5.25 GHz genutzt werden, wobei eine Sendeleistung von maximal 60 mW erlaubt ist. Beim mittleren Frequenzband muss DFS zwingend implementiert sein. Daher darf dieses Band nur benutzt werden, wenn auch DFS unterstützt wird. Im dritten Unterband sind höhere Sendeleistungen bis 1 W erlaubt. Auch hier muss DFS unterstützt sein.

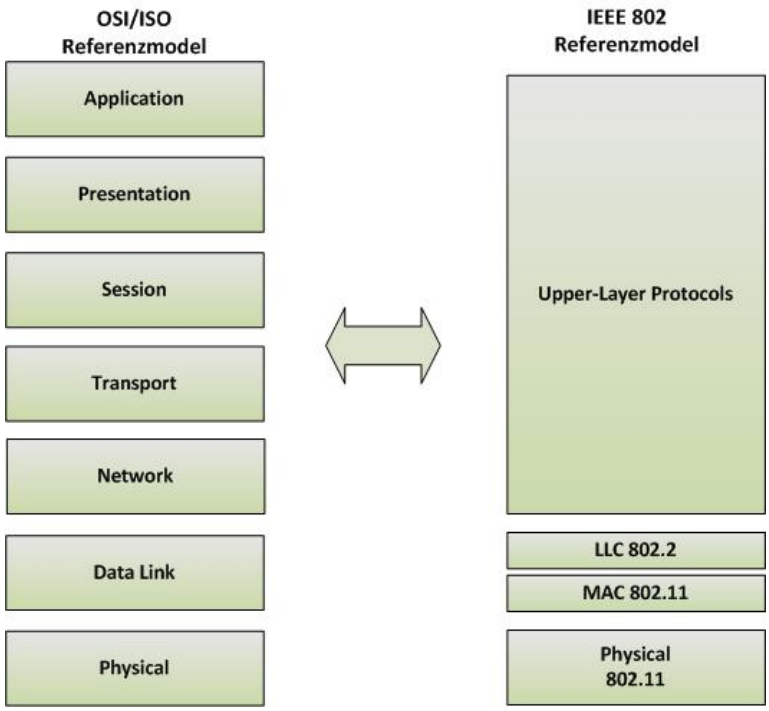
Das 5-GHz-Band stellt 19 unabhängige Kanäle bereit. Somit können im Vergleich zum 2.4-GHz-Band mehr Systeme betrieben werden, die sich gegenseitig nicht beeinflussen.

Band (GHz)	Kanalnummer	Trägerfrequenz (GHz)
5.15–5.25	36	5.180
	40	5.200
	44	5.220
	48	5.240
5.25–5.35	52	5.260
	56	5.280
	60	5.300
	64	5.320
5.47–5.725	100	5.500
	104	5.520
	108	5.540
	112	5.560
	116	5.580
	120	5.600
	124	5.620
	128	5.640
	132	5.660
	136	5.680
	140	5.700

IEEE 802.11

Die IEEE 802.11 ist eine Standardisierungsgruppe, welche sich damit beschäftigt, Standards für Funknetzwerke auf Basis des Ethernets festzulegen. Dabei befasst sie sich mit dem Physical- und dem Data-Link-Layer. Auf diesen Layers mussten für Funknetzwerke einige Neuerungen eingeführt werden.

Der Physical-Layer definiert dabei, wie die Daten über Funk zu übertragen sind. Der Data-Link-Layer ist in zwei Bereiche unterteilt. Der untere ist der MAC-Sublayer. Hier wird definiert, wie Stationen Zugriff auf das Übertragungsmedium erhalten. Der zweite Sublayer ist die LLC (Logical Link Control). Dieser Layer nimmt die Daten des Network-Layers entgegen und ist für die Bildung des Frames verantwortlich. Wenn das Frame gebildet wurde, wird es dem MAC-Sublayer übergeben und über den Physical-Layer gesendet. Der Vorteil dieses Sub-Layers ist, dass er vom jeweiligen MAC-Sublayer unabhängig ist. Somit ist dieser Layer zu den verschiedenen MAC-Layers transparent. Infolge dieser Transparenz mussten für die Festlegung des 802.11-Standards lediglich der MAC- und der Physical-Layer neu definiert werden.



IEEE-802.11-PHYSICAL-LAYER

Der 802.11-Physical-Layer ist wiederum in zwei Bereiche unterteilt. Diese sind das PLCP (Physical Layer Convergence Procedure) und das PMD (Physical Medium Dependent).

Das PLCP ist eine einheitliche Schnittstelle zum MAC-Layer. Der MAC-Layer übergibt dem PLCP das Frame, welches übertragen werden muss. Das übergebene Frame muss dann vom PLCP in ein übertragbares Format gebracht werden. Dieser Sublayer bringt auch wieder Transparenz mit ein. Somit muss bei Änderungen der Übertragungstechnik nur das PMD angepasst werden.

Die Aufgabe des PMD besteht darin, die Daten in ein für die Übertragungstechnik geeignetes Format zu bringen. Dieser Layer ist von der jeweiligen verwendeten Übertragungstechnik abhängig. Beispiele hierzu sind DSSS oder OFDM. Des Weiteren ermöglicht das PMD die Übertragung der Daten zwischen den Stationen. Daher moduliert es die zu sendenden Daten. Der Empfänger demoduliert diese und gibt sie dem PLCP-Layer weiter. Beim IEEE 802.11 besteht das Übertragungsmedium aus elektromagnetischen Wellen, die entweder im 2.4-GHz- oder im 5-GHz-Frequenzband übertragen werden.

FHSS (FREQUENCY HOPPING SPREAD SPECTRUM)

Mit FHSS wird die Signalspreizung durch den ständigen Wechsel von Frequenzen erreicht. Dazu wird der 2.4-GHz-Bereich in 79 Frequenzunterbänder (auch Kanäle genannt) aufgeteilt, wobei jedes Unterband 1 MHz breit ist. Der Wechsel der Frequenzen wird als Frequenz-Hopping bezeichnet. Dabei wird nach einer gewissen Zeitspanne die Frequenz gewechselt und anschliessend werden auf dieser Frequenz die Daten weiter übertragen. Die Zeitspanne des Frequenz-Hoppings ist von der ETSI festgelegt worden. Eine Frequenz darf für maximal 400 ms belegt werden, bevor sie gewechselt werden muss. Des Weiteren muss der Abstand zwischen der benutzten und der neuen Frequenz mindestens 6 MHz betragen.

Der Algorithmus zum Wechseln der Frequenz wird als Hopping-Sequenz bezeichnet. Es handelt sich hierbei um eine vordefinierte Liste, welche die Reihenfolge der zu benutzenden Frequenzen bestimmt. Insgesamt gibt es im IEEE 802.11 drei verschiedene Hopping-Sequenzen, die als Hopping-Sets bezeichnet werden. Stationen, welche untereinander Daten austauschen möchten, müssen zwingend dasselbe Hopping-Set verwenden. Ansonsten können die Daten nicht empfangen werden. Es ist aber möglich, dass trotz unterschiedlichen Hopping-Sets zwei Sender zeitgleich auf derselben Frequenz ihre Daten senden. Dadurch kommt es zur Kollision und die Daten müssen neu übertragen werden. Folgende Hopping-Sets wurden für die Verwendung in Europa von der IEEE 802.11 definiert:

Set	Kanäle
1.	0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75
2.	1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76
3.	2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77

DSSS (DIRECT SEQUENCE SPREAD SPECTRUM)

DSSS ist ein Verfahren, welches im 802.11- und 802.11b-Standard eingesetzt wird. DSSS basiert auf dem 2.4-GHz-Frequenzband, welches in 13 Kanäle unterteilt ist. Im Gegensatz zu FHSS sendet eine Station hierbei immer über denselben Kanal.

DSSS spreizt das schmalbandige Signal bei der Datenübertragung über einen grösseren Frequenzbereich. Der breitere Frequenzbereich wird allerdings kompensiert, indem auf diese Art und Weise eine geringere Sendeleistung benötigt wird. Störeinflüsse sind dagegen meistens schmalbandig. Durch die Spreizung wird verhindert, dass durch Störeinflüsse das gesamte Signal gestört wird. Vielmehr wird so lediglich ein Teil des Signals gestört.

Die Spreizung des Signals wird unter Verwendung eines Spreiz-Codes, des Barker-Codes, erreicht. Der Barker-Code ist ein Codierungsschema, welcher für die Spreizung des Signals im 802.11b-Standard verwendet wird. Beim Barker-Code wird jedes einzelne Informationsbit durch eine Bitsequenz von elf Bits ersetzt. Folgende Bitsequenz wird im 802.11b-Standard angewendet: „11100010010“. Um ein Informationsbit zu übertragen, müssen somit elf Bits übertragen werden. Dieser Code wird auch PN-Code (Pseudo-Noise-Code) genannt. Die Bitsequenz wird als Chirp bezeichnet. Beim Senden nimmt der Sender ein Informationsbit nach dem anderen und ersetzt jedes Bit mit dem entsprechenden Chirp. Das führt dazu, dass jedes Informationsbit durch ein Chirp ersetzt wird. Danach wird der Chirp mit dem jeweiligen Informationsbit logisch verknüpft (XOR) und daraus resultiert dann das Signal, welches übertragen wird. Der Empfänger nimmt das Signal entgegen und verknüpft es mit einem logischen XOR mit den Chirps. Als Resultat erhält er dann die gesendete Bitfolge.

Signal	1	0
Chirp	10110010	10110010
XOR	11111111	00000000
resultierendes gespreiztes Signal, das gesendet wird	00101101	10110010

gespreiztes Signal, das empfangen wird	00101101	10110010
Chirp	10110010	10110010
XOR	11111111	00000000
resultierendes Signal	1	0

In diesem Beispiel wurde eine Chiplänge von acht Bits verwendet. Dieses wird mit dem Signalwert XOR genommen und man erhält ein acht Bit langes Signal. Somit wird absichtlich Redundanz eingefügt. Der Grund dafür ist, dass das Signal bei der Übertragung aufgrund von Störeinflüssen wie Rauschen verändert werden kann. Durch die hinzugefügte Redundanz ist es trotzdem noch möglich, das Signal richtig zu empfangen. Dies ist allerdings nur gewährleistet, wenn mehr korrekte als falsche Bits vorhanden sind. Sobald mehrheitlich falsche Bits eintreffen, resultiert ein anderer XOR-Wert, welcher nicht mehr aus lauter Einsen oder Nullen besteht. Wenn dies der Fall ist, wird einfach die Anzahl an Einsen und Nullen aufsummiert. Diejenige Summe, die grösser ist, wird dann als resultierender Signalwert genommen. Beim DSSS-Verfahren ist somit eine Fehlinterpretation möglich. Der

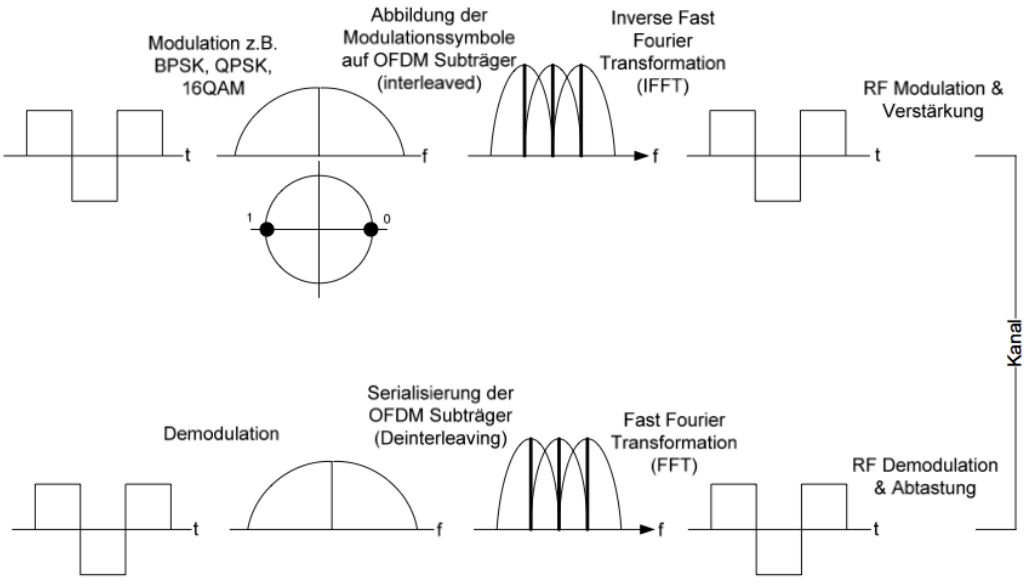
Effekt ist dann, dass eine Null vom Sender gesendet wurde, die aber beim Empfänger als eine Eins interpretiert wird. Dies wird im folgenden Beispiel veranschaulicht:

Signal	1	0
Chirp	10110010	10110010
XOR	11111111	00000000
resultierendes gespreiztes Signal, das gesendet wird	00101101	10110010

gespreiztes falsches Signal, das empfangen wird	00010010	10101101
Chirp	10110010	10110010
XOR	10100000	00011111
resultierendes Signal	0	1

OFDM (ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING)

Bei OFDM handelt es sich um ein Modulationsverfahren, welches in den neusten WLAN-Standards eingesetzt wird. Dabei werden die Kanäle in Unterkanäle aufgeteilt. Dadurch werden breitbandige Signale in schmalbandige orthogonale Signale umgewandelt. Da normalerweise ein WLAN-Kanal 20 MHz breit ist, wird dieser Kanal in 52 Unterkanäle aufgeteilt. Über diese Unterkanäle findet dann die Datenübertragung statt. Die Unterkanäle stehen orthogonal zueinander. Das heisst, dass die Amplituden der Nachbarkanäle an der Trägerfrequenz genau Null sind. Somit stören sich die Unterkanäle gegenseitig nicht. Die einzelnen OFDM-Signale werden über die Inverse Fast Fourier Transformation (IFFT) erzeugt. Durch die IFFT wird das Frequenzsignal in ein Zeitsignal umgewandelt. Das Zeitsignal ist dabei die Summe aller Sinuskurven der Unterkanäle. Dieses Zeitsignal wird dann über das Funkmedium übertragen. Beim Empfänger wird das Zeitsignal mittels Fast Fourier Transformation (FFT) wieder in ein Frequenzsignal umgewandelt. Dabei entstehen wieder die einzelnen orthogonalen Frequenzensignale.



IEEE-802.11-MAC-LAYER

Die Aufgabe des MAC-Layers ist die Bildung eines Frames sowie die Steuerung des Zugriffs auf das Übertragungsmedium. Das Funkmedium ist ein sogenanntes „shared medium“. Das bedeutet, dass alle Stationen, welche über dieses Medium senden möchten, sich dieses teilen müssen. Würden mehrere Stationen zeitgleich ihre Daten senden, so werden sich die Signale überlagern und es käme zu Kollisionen. Infolge der Kollisionen müssten die Daten wiederholt gesendet werden, bis sie auch beim Empfänger ankommen würden. Dies hat einen enormen Einfluss auf die Performance und es muss deshalb sichergestellt werden, dass es zu keinen Kollisionen kommen kann. Dieses Ziel wird durch das Zugriffsverfahren CSMA/CA sichergestellt, welches im Folgenden näher beschrieben wird.

ZUGRIFFSVERFAHREN CSMA/CA

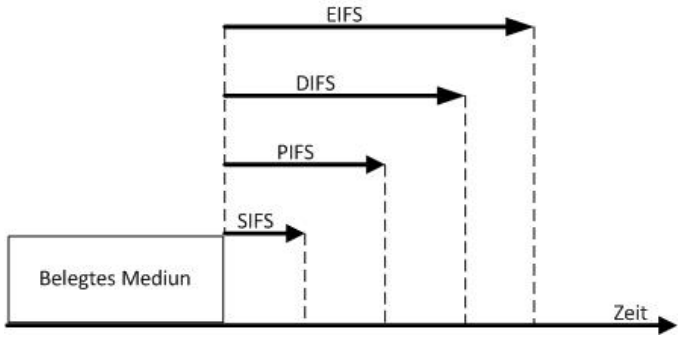
WLANs benutzen ein vom kabelgebundenen Ethernet abgeleitetes Zugriffsverfahren. Dieses Verfahren trägt den Namen „Carrier Sense Multiple Access with Collision Avoidance“. Anders als im kabelgebundenen Ethernet werden im WLAN Kollisionen nicht erkannt, sondern vermieden. Dies ist deshalb so, weil im WLAN-Bereich nicht die Möglichkeit besteht, gleichzeitig Daten zu senden und zu empfangen. Diese Einschränkung führt dazu, dass den teilnehmenden Stationen zusätzliche Informationen zur Verfügung gestellt werden müssen. Um Kollisionen zu vermeiden, wird ein Timer verwendet, der als NAV (Network Allocation Vector) bezeichnet wird. Über diesen Timer wird festgelegt, wie lange das Medium reserviert ist, bis die zu übertragenden Daten übermittelt wurden. Dieser NAV wird in jedem Frame mitgesendet und von allen teilnehmenden Stationen interpretiert und verwaltet. Der NAV-Wert ist im IEEE-802.11-Frame-Header enthalten und trägt den Namen „Duration/ID“-Feld. Da alle Stationen diese Information erhalten, sind sie in der Lage, zu erkennen, wie lange das Medium belegt ist. Erst wenn der NAV abgelaufen und das Medium frei ist, wird eine Station versuchen, auf das freie Medium zuzugreifen, um Daten zu senden. Der NAV-Wert wird auf allen Stationen ständig aktualisiert, sobald wieder ein Frame empfangen wurde.

ACKNOWLEDGEMENT

Dennoch wäre es noch möglich, dass Kollisionen auftreten. Aus diesem Grund wird beim WLAN der erfolgreiche Empfang eines Frames vom Empfänger mit einem Acknowledgement-Frame bestätigt. Dieses Frame ist 14 Byte lang und enthält lediglich einen verkürzten Header ohne Datenteil. Trifft beim Sender keine Empfangsbestätigung ein, so wird nach einer gewissen Zeitspanne das Frame erneut ausgesendet. Diese Zeitspanne wird durch den sogenannten Backoff-Algorithmus berechnet und liefert eine Zufallszeit, während der zugewartet werden muss, bis das nächste Frame gesendet werden darf. Die Frage stellt sich dabei, was alles bestätigt werden muss. Dabei wird zwischen den verschiedenen Frame-Typen unterschieden. Es wird nur der Empfang von Unicast-Frames bestätigt. Eine Empfangsbestätigung für Broadcast- bzw. Multicast-Frames ist wenig sinnvoll, da ein Sender ja nicht weiss, welche Stationen das Frame empfangen haben.

INTER FRAME SPACING

Wie in den vorherigen Abschnitten erklärt wurde, weiss jede Station durch das Verwalten des NAV, wie lange das Medium bei einer Frame-Übertragung belegt ist. Daher die Zeit, die nötig ist, bis das Frame beim Empfänger angelangt. Wenn es sich dabei um ein Unicast-Frame handelt, wird der Erhalt des Frames vom Empfänger bestätigt. Bis zum Erhalt der Empfangsbestätigung beim Sender dauert es eine gewisse Zeit. Diese Zeitspanne umfasst die Bearbeitungszeit beim Empfänger, die Generierung eines Acknowledgement-Frames sowie die Übermittlungszeit. Während dieses Zeitraums muss gewährleistet sein, dass keine andere Station das Medium bereits für sich belegt hat, um Daten zu senden. Aus diesem Grund haben Empfangsbestätigungen beim Zugriff auf das Medium eine höhere Priorität als zum Beispiel Daten-Frames. Die Sicherstellung dieser Prioritäten wird über verschiedene Zeitabstände zwischen zwei aufeinanderfolgenden Frames realisiert, welche als IFS (Inter Frame Spacing) bezeichnet werden. Die Prioritäten hängen von den jeweiligen Frame-Typen ab. Somit erhalten Frames, die über eine höhere Priorität verfügen, eine kürzere Zugriffszeit auf das Medium als niedrig priorisierte Frames.



In der obigen Abbildung sind die unterschiedlichen IFS-Typen dargestellt. Der IEEE-802.11-Standard verwendet vier verschiedene Typen, welche nun genauer beschrieben werden:

- **SIFS:** Short Inter Frame Space stellt die höchste Priorität dar. Das bedeutet, dass Frames, welche nach dem SIFS übertragen werden, bevorzugt werden. Typische Frames, die nach dem SIFS übertragen werden, sind Acknowledgement- und Clear-to-Send-Frames.
- **PIFS:** Point Inter Frame Space wird von Stationen verwendet, die PCF unterstützen. Dies wird hier nicht näher erläutert, da es für diese Arbeit keine Relevanz besitzt.
- **DIFS:** Distributed Inter Frame Space legt den zeitlichen Mindestabstand fest, wie lange eine Station warten muss, bevor sie damit beginnen darf, ihre Daten zu senden. Das heisst, dass eine Station eine DIFS-Zeitspanne lang warten muss, bevor sie einen erneuten Zugriff auf das Medium versuchen darf, um ihre Daten zu senden.
- **EIFS:** Es kann vorkommen, dass ein Frame bereits ausgesendet wird, aber der MAC-Layer dem Physical-Layer ein fehlerhaftes Frame übergeben hat. Wenn das der Fall ist, unterbricht der Physical-Layer die Übertragung dieses Frames. Aufgrund des bereits empfangenen NAV-Wertes müssten alle Stationen für diese Zeitdauer warten, obwohl keine Daten mehr gesendet werden und das Medium daher frei ist. Dies würde sich natürlich negativ auf die Geschwindigkeit auswirken. Damit die Stationen bei einem Übertragungsabbruch nicht die ganze NAV-Zeit abwarten müssen, bevor sie wieder auf das Medium zugreifen dürfen, wird der Extended Inter Frame Space verwendet. Sobald der Physical-Layer eine fehlerhafte Übertra-

gung eines Frames unterbricht, dürfen die vorhandenen Stationen nach Ablauf eines EIFS wieder auf das Medium zugreifen.

Die Länge dieser IFS-Werte kann entsprechend berechnet werden. Die Werte für SIFSTime, SlotTime, Präambel- und Physical-Layer-Header-Länge sind durch den jeweiligen Standard vorgegeben und werden aufgrund des eingesetzten Physical-Layers (OFDM, DSSS, OFDM + DSSS und Frequenzband) bestimmt.

DIFS = SIFSTime + 2xSlotTime
PIFS = SIFSTime + SlotTime
EIFS = SIFSTime + DIFS + (8 x ACK-Länge)+Präambel-Länge + Physical-Layer-Header-Länge

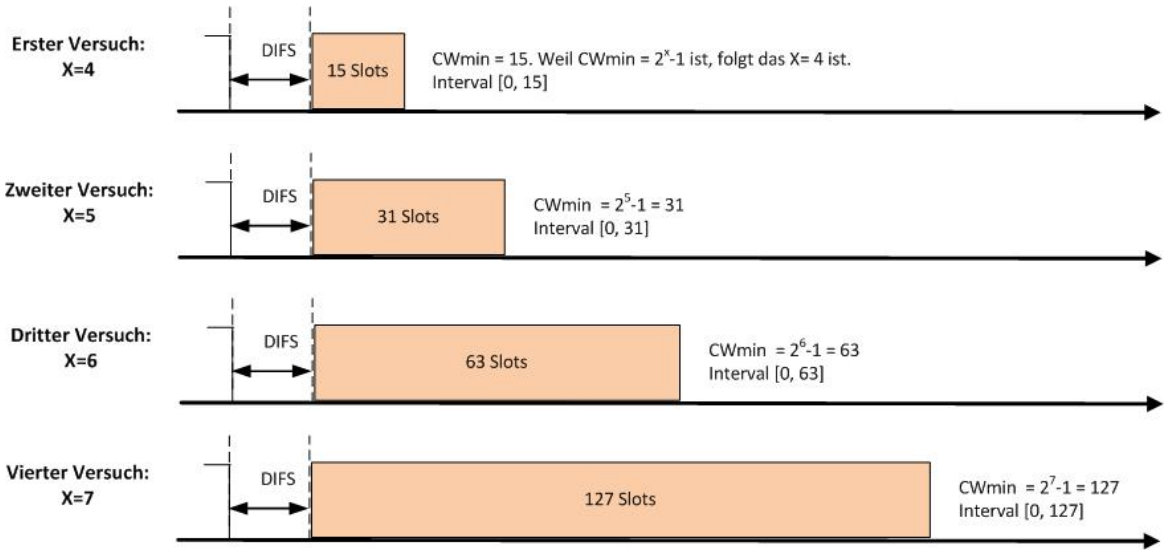
BACKOFF-ALGORITHMUS

Der Backoff-Algorithmus wird verwendet, um sicherzustellen, dass nicht alle Stationen nach einem DIFS zeitgleich auf das Medium zugreifen. Ansonsten würden zwangsläufig Kollisionen entstehen. Dieser Algorithmus wird von jeder Station berechnet, bevor diese versucht, auf das Medium zuzugreifen. Dabei handelt es sich um eine Multiplikation der SlotTime mit einer Zufallszahl.

Backoff-Zeit = Zufallszahl(CW) x SlotTime

CW ist eine ganzzahlige Zufallszahl aus dem Intervall [0, CW]. Das CW ist ein Wert zwischen CWmin und CWmax. Diese zwei Zahlen sind durch den Physical-Layer spezifiziert. CWmin und CWmax werden durch die Formel 2^x-1 berechnet. Die Variable x wird zu Beginn durch die Formel $log_2(CWmin) -1$ bestimmt. Möchte nun eine Station auf das Medium zugreifen, bestimmt sie zufällig einen Wert aus dem Intervall [0, CWmin]. Dieser zufällig ausgewählte Wert wird mit der SlotTime multipliziert und dies ergibt einen Zeitslot. Innerhalb dieses Zeitslots darf eine Station versuchen, auf das Medium zuzugreifen. Falls die Station keinen Zugriff auf das Medium erhält, weil bereits eine andere Station darauf zugreift, erhöht die Station die Variable x um 1. Durch das Inkrementieren der Variable x ergibt sich nach jedem Fehlversuch ein grösseres Intervall, in dem die Station versuchen kann, auf das Medium zuzugreifen. Dies geschieht solange, bis das CWmax erreicht wurde. Durch dieses Verfahren gibt es eine gute Wahrscheinlichkeitsverteilung, dass nicht alle Stationen zur gleichen Zeit auf das Medium zugreifen und es somit zu weniger Kollisionen kommt.

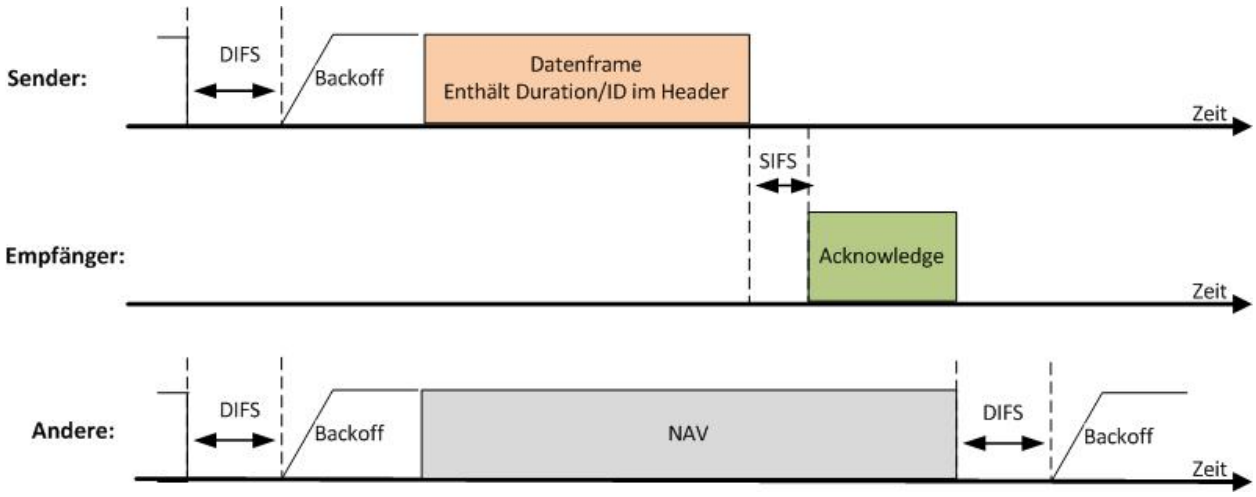
Dieses Beispiel veranschaulicht den Vorgang beim 802.11g-Standard, wenn eine Station mehrfach versucht, auf das Medium zuzugreifen.



ÜBERTRAGUNG EINES DATENFRAMES

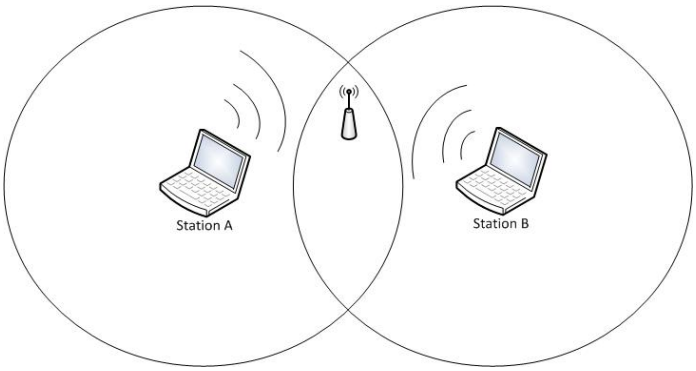
In der unteren Abbildung ist eine typische Übertragung eines Frames dargestellt. Alle Stationen warten für eine Zeitdauer von DIFS, bevor sie versuchen, auf das Medium zuzugreifen. Danach wird die Backoff-Zeit berechnet.

Nachdem beim Sender die Wartezeit aufgrund des Backoff-Algorithmus abgelaufen ist, kann er mit der Aussendung des Frames beginnen. Zeitgleich merken alle anderen Stationen, dass ein Frame ausgesendet wird, und setzen aufgrund der im Header enthaltenen Duration/ID lokal ihren NAV. Der NAV setzt sich aus der Duration/ID, der SIFS-Zeit sowie der Acknowledgement-Frame-Übertragungszeit zusammen. Somit wissen alle Stationen, wie lange das Medium besetzt ist und wann der Sendeprozess wieder von vorne beginnt.



HIDDEN-STATION-PROBLEM

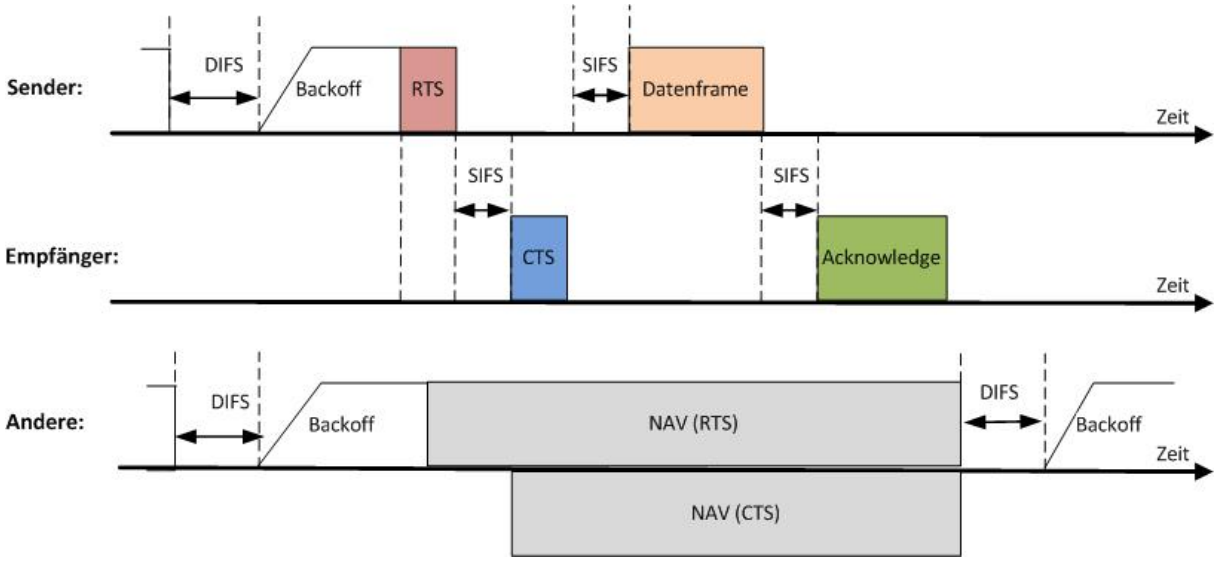
Das Hidden-Station-Problem ist ein häufiges Problem im WLAN-Bereich. Es ist in der untenstehenden Zeichnung bildlich dargestellt. Hierbei gibt es zwei Stationen, welche an einen Access Point assoziiert sind. Jeder WLAN-Adapter in der Station hat eine gewisse Reichweite. Wegen der begrenzten Reichweite einer Station kann es vorkommen, dass man nicht alle Stationen im WLAN erkennen kann. Somit kann es sein, dass Station A Station B nicht erkennt. Durch das Nichterkennen der Stationen untereinander kann es dazu kommen, dass beiden Stationen das Medium als frei erscheint. Das Problem ist nun, dass beide Stationen zeitgleich versuchen, ein Frame zu senden. Dies kann eintreffen, da Station A nicht erkennt, dass Station B bereits ein Frame an den Access Point sendet und das Medium daher schon belegt ist. Somit kommt es zu Kollisionen. Dieses Problem hat einen enormen Einfluss auf die Performance eines WLAN.



Dieses Problem wurde vom IEEE-802.11-Gremium erkannt und dieses hat deshalb einen Mechanismus zur Vermeidung dieses Problems implementiert. Dessen Name lautet RTS/CTS-Mechanismus. Der Vorgang dieses Mechanismus ist folgender:

1. Station A prüft, ob das Medium frei ist. Wenn das Medium frei ist, sendet es ein RTS-Frame (request to send) zum Empfänger. In unserem Beispiel ist das der Access Point.
2. Nach Erhalt des RTS-Frames sendet der Access Point ein CTS-Frame (clear to send).
3. Dieses Frame wird von allen Stationen, die am Access Point assoziiert sind, erkannt. Die Stationen aktualisieren ihren NAV, den sie durch das CTS-Frame erhalten haben. Somit erkennen alle Stationen, die in der Funkzelle sind, dass das Übertragungsmedium belegt ist, und versuchen nicht, auf das Übertragungsmedium zuzugreifen.

Durch den RTS/CTS-Mechanismus ist somit gewährleistet, dass es zu keinen Kollisionen bei der Übertragung von Daten kommt. Nichtsdestotrotz besteht immer noch die Möglichkeit, dass die RTS/CTS-Frames kollidieren. Da aber diese Frames relativ kurz sind (RTS 20 Byte, CTS 14 Byte), ist das Übertragungsmedium dabei nur für die Dauer eines SIFS belegt. Diese Dauer ist viel kürzer, als wenn es zu einer Kollision von Datenframes kommt. Bei einer Kollision von Datenframes wäre das Medium für die gesamte Dauer der Datenframe-Übertragung belegt. Dies würde unnötig Zeit beanspruchen, was sich wiederum negativ auf die Performance auswirken würde. In der unteren Abbildung ist die Übertragung eines Frames unter Verwendung des RTS/CTS-Mechanismus dargestellt.

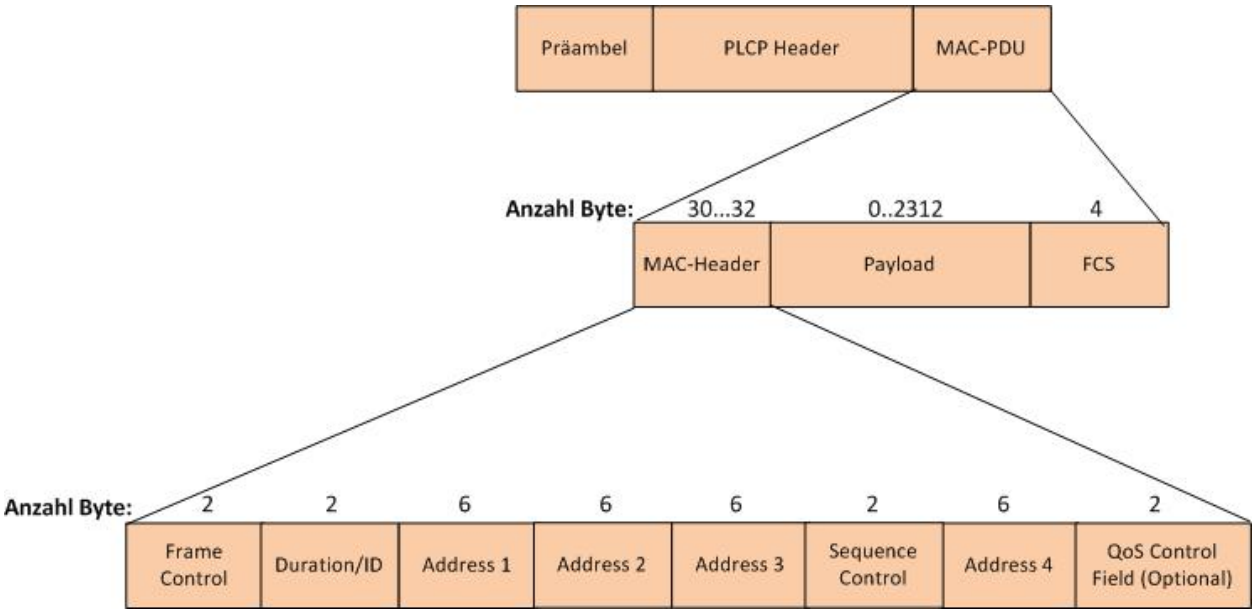


802.11 FRAME-FORMAT

Für WLANs wurde ein neues Frame-Format definiert. Dies ist notwendig, da bei der Übertragung von Daten zusätzlich noch Kontroll- und Managementinformationen ausgetauscht werden müssen, um eine reibungslose Kommunikation zu gewährleisten. Daher gibt es neben den Daten-Frames auch Kontroll- und Informations-Frames.

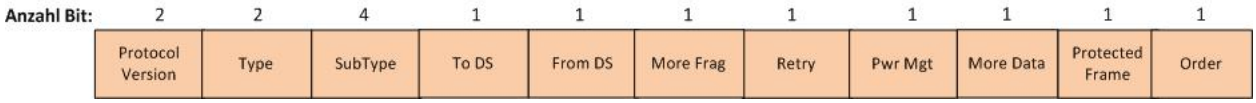
DATEN-FRAME

In der untenstehenden Abbildung ist ein generelles 802.11-Daten-Frame dargestellt. Ein Frame besteht aus einem MAC-Header, dem Payload (Nutzdaten) und einer FCS (Frame Check Sequence). Der MAC-Header hat eine Länge zwischen 30 und 32 Byte. Je nachdem, ob QoS genutzt wird, ist der Header bis zu 32 Byte gross. Der Payload ist variabel und hat eine maximale Länge von 2312 Byte. In diesem Frame sind die Daten von den höheren Layers enthalten. Am Schluss wird eine FCS hinzugefügt, welche für die Fehlererkennung und -korrektur benötigt wird.



FRAME CONTROL

In diesem Frame sind verschiedene Informationen enthalten, bei denen es sich hauptsächlich um Kontrollinformationen handelt. Der Aufbau ist folgendermassen:



Feld	Beschreibung
Protocol Version	Dies ist bei allen WLAN-Standards auf 0x00 gesetzt.
Type	Hier wird angegeben, um was für ein Frame es sich handelt. Dabei wird zwischen drei Typen unterschieden: • Management-Frame: 00 • Kontroll-Frame: 01 • Daten-Frame: 10.
Subtype	Für jeden Frame-Typ gibt es weitere Untertypen, welche in diesem Feld angegeben werden. Beispiele dazu sind Daten-Frames, ACK-, RTS- und CTS-Frames.
To DS / From DS	Diese Bits legen fest, welchen Weg das Frame bei der Übertragung gehen soll. • innerhalb einer IBSS: 00 • Frame wird von AP an Station gesendet: 01 • Frame wird von Station an AP gesendet: 10 • Frame wird zwischen APs gesendet: 11
More Frag	Wenn dieses Bit auf 1 gesetzt ist, dann erkennt die Station, dass noch weitere Fragmente empfangen werden, die zur selben Nachricht gehören.
Retry	Dieses Bit wird auf 1 gesetzt, wenn das Frame zum zweiten Mal gesendet wird.
Power Management	Ist dieses Bit auf 1 gesetzt, dann wird einer Station signalisiert, dass sie in den Stromsparmodus übergehen kann, weil beispielsweise keine weiteren Frames folgen.
More Data	Signalisiert einer Station, dass sie noch weitere Frames erhalten wird. Dadurch wird die Station nicht auf den Stromsparmodus wechseln.
Protected Frame	Gibt an, ob die Nutzdaten verschlüsselt sind oder nicht. Eine 1 bedeutet, dass sie verschlüsselt wurden.
Order	Falls es sich bei den Frames um einzelne Fragmente handelt, wird mit diesem Bit angezeigt, ob diese nach Erhalt ihrer Reihenfolge an die oberen Layers übergeben werden sollen.

DURATION/ID

Das Duration/ID-Feld ist vom jeweiligen Frame-Typ und Subtyp abhängig. Je nachdem, wie das Frame übertragen wird, sind darin andere Werte enthalten. Laut IEEE-802.11-2007-Standard sind folgende Duration/ID-Möglichkeiten vorhanden:

Bits 0 -13	Bit 14	Bit 15	Beschreibung
0 – 32'767		0	Zeit in µs, welche benötigt wird, um das Datenframe zu übertragen.
0	0	1	Fester Wert, der angibt, wie lange ein Frame mittels CFP übertragen wird.
1 – 16'383	0	1	reserviert
0	1	1	reserviert
1 - 2007	1	1	AID innerhalb eines PS-Poll-Frames
2008 – 16'383	1	1	reserviert

ADDRESS

Anders als beim normalen Ethernet sind beim 802.11-MAC-Header bis zu vier verschiedene Adressfelder vorhanden. Bei den Adressen handelt es sich auch hier um MAC-Adressen. Diese Adressen dienen dazu, BSSID-, Quell-, Ziel-, übertragende und empfangende Station identifizieren zu können. Welche Adresse wann verwendet wird, hängt davon ab, wie die Frames übertragen werden. Dies ist in der folgenden Tabelle ersichtlich:

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	Empfänger	Sender	BSSID	
0	1	Empfänger	BSSID	Sender	
1	0	BSSID	Sender	Empfänger	
1	1	Empfangender Access Point	Sendender Access Point	Empfänger	Sender

SEQUENCE CONTROL

Wenn längere zusammenhängende Daten übertragen werden, deren Länge diejenige der MTU übersteigt, dann müssen diese Daten vor dem Senden unterteilt und in mehrere Frames gepackt werden. Dieser Vorgang wird als Fragmentierung bezeichnet. Die einzelnen Frames, welche zu einem Datenstück gehören, werden als Fragmente bezeichnet. Der Empfänger fügt die erhaltenen Fragmente wieder zu einem ganzen Datenstück zusammen, sodass das Datenstück wieder als Ganzes vorhanden ist. Für die Steuerung der Fragmentierung wird das Sequence-Control-Field verwendet. Das Sequence-Control-Fieldist in zwei Bereiche aufgeteilt, Fragment Number und Sequence Number. Die Fragment Number ist bei allen Fragmenten, welche zu einem Datenstück gehören, gleich. Durch diese Nummer können sie als zusammenhängende Daten identifiziert werden. Die Sequence Number dient zur Durchnummerierung der einzelnen Fragmente, sodass sie beim Empfänger wieder in der richtigen Reihenfolge zusammengesetzt werden können.

Die Fragment Number ist beim ersten Fragment auf 0 gesetzt und wird bei jedem weiteren Fragment um 1 inkrementiert. Die Sequence Number startet bei 0 und wird bei jedem weiteren Fragment um 1 inkrementiert und mittels der Modulo-4096-Operation gebildet.

QOS CONTROL

Das QoS-Control-Field ist in Datenframes enthalten, welche über QoS übertragen werden.

Bits 0..3	Bit 4	Bits 5..6	Bits 7	Bit 8..15	Frame-Typ
TID	EOSP	ACK-Policy	Reserved	TXOP-Limit	QoS CF-Poll-Frames, die der HC überträgt
TID	EOSP	ACK-Policy	Reserved	AP-PS-Puffergrösse	QoS-Daten, welche durch HC gesendet werden
TID	0	ACK-Policy	Reserved	TXOP-Duration-Anfrage	Datenframes, welche von Stationen gesendet werden, die QoS nicht unterstützen
TID	1	ACK-Policy	Reserved	Warteschlangengrösse	

Die verwendeten Subfelder werden nun genauer erläutert.

TID (Traffic Identification)

Die TID identifiziert die TC (Traffic Category), zu welcher die MSDU gehört. Dabei gibt es folgende Felder:

Bits 0..3	Zugriff	Benutzung
0 – 7	EDCA	User-Priorisierung
8 – 15	TSID	Priorisierung durch speziellen Verkehr

EOSP (End of Service Period)

Ist dieses Bit auf 1 gesetzt, signalisiert der Access Point der Station, dass er in den Power-Save-Modus gehen kann.

ACK-Policy

Die ACK-Policy definiert, wie Bestätigungen gehandhabt werden.

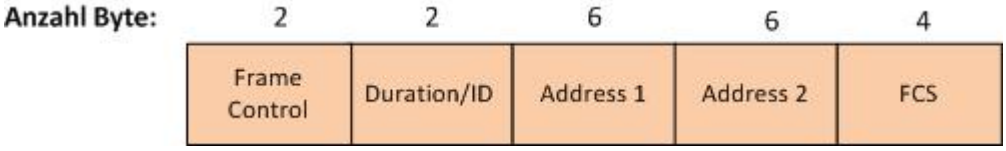
Bits 5:	Bit 6:	Bedeutung
0	0	Es wird das normale ACK verwendet. Das heisst, jedes Frame wird nach einem SIFS bestätigt.
1	0	Es soll kein ACK verwendet werden (erst ab 802.11e möglich).
0	1	kein explizites ACK verlangt
1	1	Es wird Block-ACK verwendet.

KONTROLL-FRAMES

Die Kontroll-Frames werden für den Zugriff auf das Medium verwendet. Sie stellen sicher, dass die Übertragung der Daten zuverlässig ist. Zu diesen Frames gehören beispielsweise RTS/CTS-Frames, ACK-Frames und noch weitere.

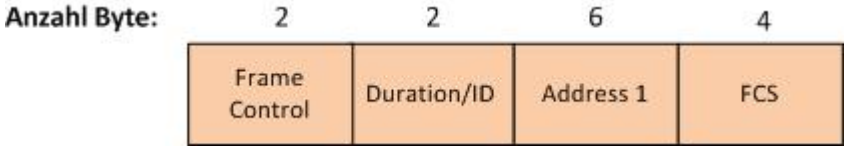
RTS

Das RTS-Frame wird verwendet, um das Hidden-Station-Problem zu vermeiden. Dieses Frame hat eine Länge von 20 Byte. Die Duration/ID beinhaltet die Dauer in µs, die benötigt wird, um ein CTS-Frame, Daten-Frame, ACK-Frame und drei SIFS zu übertragen. Das Address-1-Feld beinhaltet die MAC-Adresse des Empfängers und das Adress-2-Feld die MAC-Adresse des Senders.



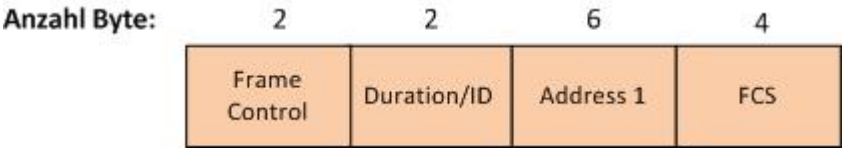
CTS

Beim Empfang eines RTS-Frames wird von Empfänger ein CTS-Frame zurückgesendet, sobald das Medium nicht belegt ist. Die Länge des CTS-Frames beträgt 14 Byte. Die Duration/ID enthält wiederum die Dauer in µs, die benötigt wird, um das Daten-Frame, das ACK-Frame und zwei SIFS zu übertragen. Die Address 1 entspricht der Senderadresse des empfangenen RTS-Frames.



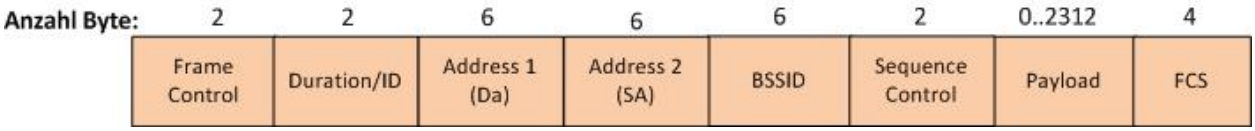
ACK

Um den Empfang eines Unicast-Frames zu bestätigen, wird das ACK-Frame zurückgesendet. Dieses Frame ist 14 Byte lang. Bei der Duration/ID gibt es zwei unterschiedliche Varianten. Handelt es sich um ein Datenframe, so ist die Duration/ID auf 0 gesetzt. Dies signalisiert dem Sender, dass die Übertragung abgeschlossen ist. Wenn ein einzelnes Fragment empfangen wurde, dann ist die Duration/ID die restliche Zeit in µs, die benötigt wird, um die restlichen Fragmente zu übertragen. Im Adress-1-Feld ist die MAC-Adresse der Station enthalten, an die das ACK-Frame zurückgesendet wird.



MANAGEMENT-FRAMES

Management-Frames dienen zur Verwaltung von WLANs. Dazu gehören die An- und Abmeldung einer Station beim Access Point und das Auffinden von vorhandenen Access Points. Im Gegensatz zu den Kontroll-Frames haben Management-Frames einen generellen Frame-Header. Einzig der Payload ist bei den verschiedenen Arten von Management-Frames unterschiedlich.



Im Weiteren werden nur diejenigen Arten von Management-Frames genauer betrachtet, welche für diese Arbeit relevant sind. Dazu gehören der Association Request, die Association Response, Beacon-Frames und Probe-Request-/-Response-Frames.

ASSOCIATION REQUEST

Versucht sich eine Station mit einem Access Point verbinden, so sendet sie ein Association-Request-Frame an den Access Point. Im Payload sind dabei verschiedene Informationen enthalten.

Information	Beschreibung
Capability	Hier wird angegeben, ob Standarderweiterungen unterstützt werden, z.B: ESS, CF-Pollable, Short Preamble, QoS, DSSS-OFDM, Block-, Delayed Acknowledgement.
Listen Interval	
SSID	Name des entsprechenden Funknetzes
Supported Rates	Hier sind die unterschiedlichen Datenraten aufgelistet, welche der Client unterstützt. Max. acht Datenraten.
Extended Supported Rates	Falls ein Client mehr als acht Datenraten unterstützt, werden diese in diesem Feld angegeben.
Power Capability	falls Power Management unterstützt wird
Supported Channels	Hier werden die unterstützten Kanäle aufgelistet.
RSN	Angabe, falls RSN auf der Station aktiviert ist
QoS Capability	Angabe, ob QoS von der Station unterstützt wird
Vendor Specific	eine oder mehrere herstellerspezifische Informationen

ASSOCIATION RESPONSE

Hiermit bestätigt ein Access Point die Assoziierung einer Station. Dabei sind folgende Informationen im Payload enthalten:

Information	Beschreibung
Capability	Hier wird angegeben, ob Standarderweiterungen unterstützt werden, z.B: ESS, CF-Pollable, Short Preamble, QoS, DSSS-OFDM, Block-, Delayed Acknowledgement.
Status Code	Gibt den Status der Assoziierung an. Dabei steht 0 für erfolgreich.
AID	Der Station wird eine ID zugewiesen. Durch diese ID wird z.B. das Power Management getätigt. Der Access Point kann über die AID der Station melden, dass er Frames für sie hat und die Station deshalb aus dem Standby-Modus aufwachen sollte.
Supported Rates	Hier sind die unterschiedlichen Datenraten aufgelistet, welche der Access Point unterstützt. Max. acht Datenraten.
Extended Supported Rates	Falls ein Access Point mehr als acht Datenraten unterstützt, werden diese in diesem Feld angegeben
EDCA Parameter Set	Hier werden QoS-Angaben gemacht. Z.B: die verschiedenen konfigurierten AIFS etc.
Vendor Specific	eine oder mehrere herstellerspezifische Informationen

BEACON-FRAMES

Damit eine Station über das Vorhandensein eines WLAN informiert wird, werden sogenannte Beacon-Frames von den jeweiligen Access Points ausgesendet. Diese Frames werden über eine Layer-2-Broadcast-Adresse gesendet. Somit erhalten alle Stationen, die sich in der Reichweite dieses Netzwerks befinden, diese Beacon-Frames. In den Beacon-Frames sind wesentliche Informationen über das jeweilige Netzwerk enthalten, beispielsweise der Name des WLAN (SSID), die unterstützenden Datenraten, der benutzte Kanal etc. Durch den Erhalt dieses Frames hat eine Station genügend Informationen, damit sie sich mit dem Netzwerk verbinden kann. Um sicherzustellen, dass wirklich alle Stationen, welche in der Reichweite dieses Netzwerks sind, diese Beacon-Frames auch erhalten, werden sie mit einer sehr niedrigen Geschwindigkeit ausgesendet. Meistens werden sie mit einer Übertragungsrate von 1 Mbit/s vom Access Point ausgesendet. Dies liegt daran, dass mit zunehmender Distanz die Übertragungsrate aufgrund der Dämpfung des Signals abnimmt. Eine Station kann sich an diese Dämpfung anpassen. Je schwächer das Signal ist, desto kleiner wird die Übertragungsrate bei der Station gewählt. Dieser Mechanismus bezeichnet man als ARD (Adaptive Rate Detection).

Folgende Elemente können im Beacon-Frame enthalten sein:

Information	Beschreibung
Time Stamp	dient zur Zeitsynchronisation zwischen Stationen und Access Point
Beacon Interval	Intervall in Sekunden, gibt an, wie oft Beacon-Frames ausgesendet werden
Capability	Hier wird angegeben, ob Standarderweiterungen unterstützt werden,

	z.B: ESS, CF-Pollable, Short Preamble, QoS, DSSS-OFDM, Block-, Delayed Acknowledgement
SSID	Name des Funknetzwerks
Supported Rates	Hier sind die unterschiedlichen Datenraten aufgelistet, welche der Access Point unterstützt. Max. acht Datenraten.
Frequence Hopping Sequence Set	Hier wird angegeben, welches Hopping Set zu verwenden ist.
DS Set	Hier wird der Kanal angegeben, den das WLAN benutzt.
CF Parameter Set	Dauer der CFP-Intervalle
Traffic indication map	Mit TIM kann ein Access Point einer Station, die sich im Power-Save-Modus befindet, mitteilen, dass er eine Nachricht für sie zwischengespeichert hat.
Country Code	Identifizierung der länderspezifischen Einstellungen, z.B die zu verwendenden Kanäle etc.
Power Constraint	Spezifiziert die Leistung eines Kanals. Dadurch kann die Leistung entsprechend angepasst werden.
Channel Switch Announcement	Wenn DFS verwendet wird, kann ein Access Point den Stationen mitteilen, dass ein Kanalwechsel stattfindet.
Quiet	Spezifiziert eine Zeitdauer, während der auf dem Kanal keine Informationen ausgesendet werden dürfen.
ERP Informations	Hier wird signalisiert, dass sich im BSS auch non-ERP Stationen befinden und ob der Protection-Mechanismus oder die Short Preamble verwendet werden muss.
Extended Supported Rate	Falls ein Access Point mehr als acht Datenraten unterstützt, werden diese in diesem Feld angegeben.
RSN	Aushandlung der Verschlüsselungsmethode
BSS Load	Anzeige der Auslastung der BSS
EDCA Parameter Set	Hier werden QoS-Angaben gemacht, z.B die verschiedenen konfigurierten AIFS etc.
QoS Capability	Angabe der verschiedenen QoS-Methoden
Vendor Specific	eine oder mehrere herstellerspezifische Informationen

PROBE-REQUEST

Eine Station sendet in bestimmten Zeitabständen Probe-Request-Frames aus. Diese dienen zum Auffinden von Access Points. Auch hier werden die SSID und die unterstützten Datenraten übertragen.

PROBE-RESPONSE

Ein Probe-Request wird mit einer Probe-Response beantwortet. Die Probe-Response enthält dieselben Informationen, die auch im Beacon-Frame enthalten sind. Mit der Probe-Response hat die Station genügend Informationen, um sich mit dem Access Point zu verbinden.

DER IEEE-802.11G-STANDARD

Der 802.11g-Standard erlaubt eine Bruttoübertragungsrate von bis zu 54 Mbps. Diese Übertragungsraten werden hauptsächlich aufgrund des erweiterten Physical-Layers erreicht. 802.11g benutzt neu das OFDM-Verfahren. Dabei wird ein 20-MHz-Kanal in 52 Unterkanäle unterteilt, wobei für die Signalübertragung lediglich 48 Unterkanäle benutzt werden können.

SHORT PREAMBLE

Eine Neuerung des 802.11g-Standards ist die Einführung einer verkürzten Präambel. Die IEEE-802.11b-Gruppe hatte festgestellt, dass die Präambel zu lang ist und dies unnötigen Overhead hinzufügt. Aus diesem Grund wurde eine neue Präambel definiert. Da diese eine verkürzte Variante darstellt, wird sie als „Short Preamble“ bezeichnet. Die IEEE-802.11g-Gruppe empfiehlt die Benutzung der verkürzten Präambel. Die Short Preamble wird immer im ERP-OFDM verwendet. Bei den restlichen Physical-Layers ist die Verwendung der Short Preamble von den Stationen abhängig. Unterstützen sowohl Sender als auch Empfänger die Short Preamble, so wird sie benutzt. Ansonsten wird die lange Präambel verwendet.

PHY-TYPEN

Beim 802.11g-Standard werden zwei Physical-Layer-Typen unterschieden. Diese sind:

- **ERP (Extended Rate PHY):** Dies ist der neue Physical-Layer. Dieser Layer unterstützt die höheren Datenraten bis 54 Mbps.
- **Non-ERP:** Dies ist der bisherige Physical-Layer, wie er schon im 802.11- und 802.11b-Standard verwendet wird. Mit diesem Physical-Layer werden Datenraten von 1 Mbps bis 11 Mbps unterstützt und DSSS als Spreizverfahren eingesetzt.

Zusätzlich werden im 802.11g-Standard vier verschiedene Physical-Layers unterschieden.

- **ERP-OFDM:** Dies ist der neue Modus, welcher von der IEEE-802.11g-Gruppe eingeführt wurde. Bei diesem Modus werden die Daten mithilfe des OFDM-Verfahrens übertragen. Es werden Datenraten bis 54 Mbps unterstützt.
- **ERP-DSSS:** Dieser Modus ist der alte Physical-Layer, welcher von den 802.11b-Stationen eingesetzt wird. Er erlaubt eine maximale Datenrate von 11 Mbps.
- **ERP-PBCC:** Dieser Modus ist optional und wurde von den meisten Herstellern nicht implementiert. Es wird das PBCC-22- oder PBCC-33-Codierungsverfahren eingesetzt und eine Übertragungsrate bis zu 33 Mbps unterstützt.
- **DSSS-OFDM:** Ist wie ERP-OFDM ein neuer Physical-Layer. Unterstützt das DSSS- und das ODFM-Verfahren. Dabei werden die Nutzdaten über OFDM übertragen. Um die Abwärtskompatibilität zu unterstützen, wird vor den Nutzdaten ein 802.11b-kompatibler Header angefügt, der mit dem DSSS-Verfahren übertragen wird. Dies stellt sicher, dass auch 802.11b-Stationen registrieren, dass ein Frame übertragen wird und das Medium deshalb belegt ist.

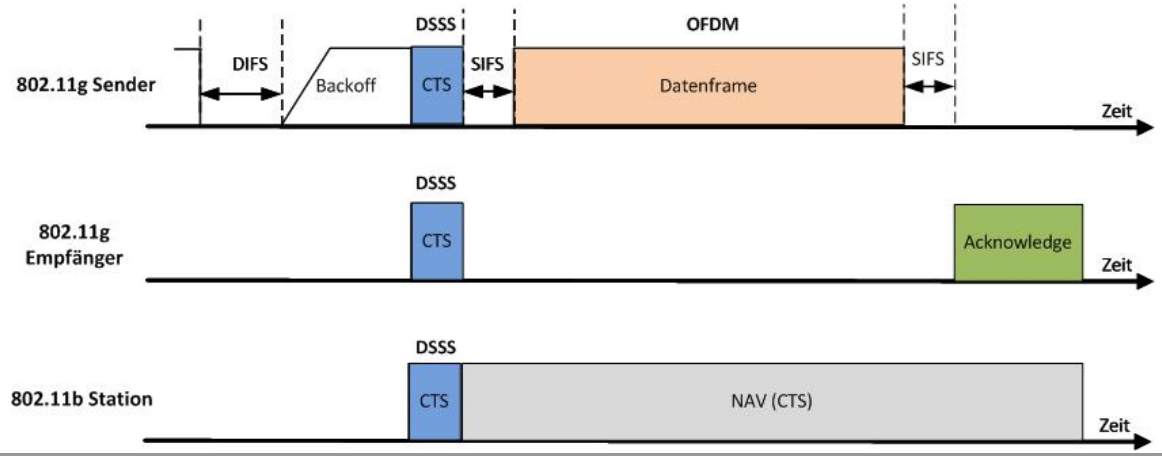
INTEROPERABILITÄT

Im 802.11g-Standard muss die Interoperabilität mit älteren Standards wie 802.11b gewährleistet sein. Denn es ist möglich, dass unterschiedliche Geräte im Netzwerk vorhanden sind. Folgende Geräte können im Netzwerk vorkommen:

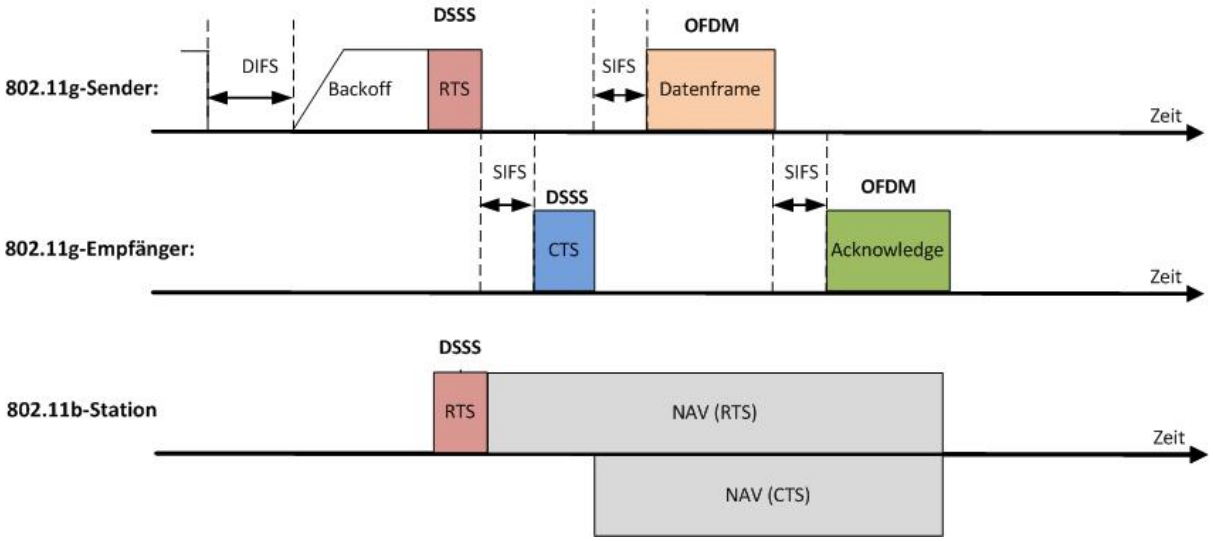
- **ERP-Stationen:** Stationen, die ERP-OFDM nach dem 802.11g Standard unterstützen.
- **Non-ERP-Stationen mit „Short Preamble“:** Stationen, welche den 802.11b-Standard unterstützen und die Short Preamble benutzen.
- **Non-ERP-Stationen mit „Long Preamble“:** Stationen, die ebenfalls nach 802.11b-Standard arbeiten, aber die lange Präambel verwenden.

Dieses Nebeneinander verschiedener Stationen kann zu Problemen führen. ERP-Stationen senden ihre Daten über ERP-OFDM. Non-ERP-Stationen unterstützen OFDM nicht. Daraus resultiert, dass diese Stationen nicht merken, dass Daten übertragen werden. Somit registrieren sie, dass das Medium frei sei, und senden ihre Daten. Dadurch kommt es zu Kollisionen. Um solche zu vermeiden, wurden verschiedene Lösungsmöglichkeiten spezifiziert. Die erste besteht darin, dass eine ERP-OFDM-Station, wenn sie ihre Daten aussendet, vor den eigentlichen OFDM-Daten einen Header einfügt, welcher mittels DSSS-Verfahren gesendet wird. Dadurch erhalten auch Non-ERP-Stationen die Information, dass das Medium belegt ist, und können ihren NAV entsprechend setzen. Die zweite Lösung basiert auf dem Protection-Mechanismus. Dabei sendet der Access Point seine Beacon-Frames mit dem DSSS-Verfahren aus. Dadurch ist sichergestellt, dass auch 802.11b-Stationen ein WLAN auffinden können. Sobald Non-ERP-Stationen mit dem Access Point assoziiert sind, wird im Beacon-Frame das Protection-Feld auf 1 gesetzt. Dadurch erfahren alle ERP-OFDM-Stationen, dass sich 802.11b-Stationen im Netzwerk befinden. Wenn das Protection-Feld im Beacon vorhanden ist, gibt es wiederum zwei Möglichkeiten, die von ERP-Stationen genutzt werden können, um die Kompatibilität zu gewährleisten:

Die erste Möglichkeit ist das CTS-to-Self-Verfahren. Dabei sendet eine ERP-Station ein CTS-Frame aus, das an die Station selber adressiert ist und den NAV-Wert beinhaltet. Dieses CTS-Frame wird mittels DSSS-Verfahren übertragen und von allen ERP- und Non-ERP-Stationen empfangen. Über den NAV-Wert erhalten die Stationen die Medienreservierungsdauer der sendenden Station und es kommt somit zu keinen Kollisionen mehr. Nach dem Empfang des eigenen CTS-Frames durch die Station werden dann die Nutzdaten über ERP-OFDM übertragen.



Die zweite Möglichkeit ist die Verwendung des RTS/CTS-Mechanismus. Wenn eine ERP-Station Daten übertragen möchte, wird das RTS/CTS-Verfahren genutzt. Dabei werden diese zwei Frames mittels DSSS übertragen. Auch hier ist die Dauer der Medienreservierung enthalten. Die non-ERP-Stationen wissen dadurch, wie lange das Medium belegt ist. Die eigentlichen Nutzdaten der ERP-Station werden anschliessend mittels OFDM-Verfahren übertragen.



PHY-PARAMETER

Unten sind die für diese Arbeit wichtigsten physikalischen Parameter des 802.11g-Standards aufgelistet:

Parameter	Wert
SlotTime:	20 µs (ERP und Non-ERP in BSS) 9 µs (nur ERP-OFDM in BSS)
SIFSTime:	10 µs
PIFSTime:	30 µs (ERP und Non-ERP in BSS) 19 µs (nur ERP-OFDM in BSS)
DIFSTime:	50 µs (ERP und non-ERP in BSS) 28 µs (nur ERP-OFDM in BSS)
Präambel-Dauer:	72 µs (ERP und non-ERP in BSS) 20 µs (nur ERP-OFDM in BSS)
Dauer für Physical-Layer-Header:	24 µs (ERP und non-ERP in BSS) 4 µs (nur ERP-OFDM in BSS)
CWmin:	15
CWmax:	1023
Maximale MPDU-Länge:	4095 Byte

DER IEEE-802.11E-STANDARD

Im 802.11e-Standard wird QoS (Quality of Service) für WLANs spezifiziert. Somit lassen sich auch im WLAN zeitkritische Daten wie Sprache oder Video übertragen. Um dies zu erreichen, wird der Verkehr klassifiziert und dann übertragen. Zusätzlich wurden noch weitere Ergänzungen gemacht, welche im Folgenden genauer erläutert werden.

EDCF (ENHANCED DISTRIBUTION COORDINATION FUNCTION)

Die Klassifizierung des Verkehrs wird über das EDCF gemacht. Dazu gibt es acht Traffic Categories (TCs). Jede dieser TCs hat jeweils unterschiedliche Priorität. Beim Zugriff auf das Medium wird diese Priorität berückichtigt. Die Priorität der verschiedenen TCs führt zu Unterschieden in der Zugriffsdauer auf das Medium. So haben höher priorisierte TCs eine kürzere Wartezeit, bis sie auf das Medium zugreifen dürfen. Jede TC erhält für eine bestimmte Zeit eine Zugriffsberechtigung auf das Medium. Diese Dauer ist als TXOP (Transmission Opportunity) definiert. Während dieser Dauer darf eine Station so viele Frames aussenden, wie möglich sind.

Für die neue Zugriffsdauer wurde ein neuer IFS bestimmt. Dies ist der AIFS (Arbitration Inter Frame Space). Der AIFS hat eine Mindestdauer von DIFS und kann individuell für jede TC verlängert werden. Nach Ablauf des AIFS wird die Backoff-Zeit abgewartet, bevor auf das Medium zugegriffen werden darf. Je höher die Priorität einer TC ist, desto kürzer ist die Backoff-Zeit. Aus diesem Grund erhalten höher priorisierte TCs vor den niedriger priorisierten TCs Zugriff auf das Medium.

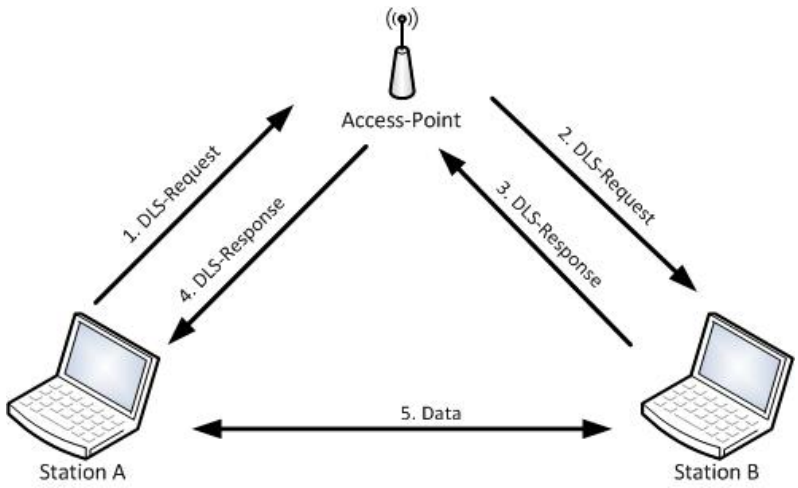
HCF (HYBRID COORDINATION FUNCTION)

HCF ist eine Erweiterung von EDCF. Dabei kommt zusätzlich ein HC (Hybrid Controller) zum Einsatz. Dieser kann jeder Station eine TXOP zuteilen und dadurch erhält die Station Zugriff auf das Medium. Die Zuteilung einer TXOP findet über den Access Point statt. Dabei pollt der Access Point mittels eines CF-Poll-Frames Stationen an und erteilt ihnen die Erlaubnis, auf das Medium zuzugreifen. Das CF-Poll-Frame wird ausgesendet, wenn das Übertragungsmedium für die Dauer eines PIFS frei ist, und enthält eine Duration/ID, welche der Station die Dauer der TXOP angibt. Dadurch erfährt eine Station, wie lange sie auf das Medium zugreifen kann. Weil ein CF-Poll-Frame immer nach einem PIFS ausgesendet wird, hat der HC die höchste Priorität. Die Aussendung der CF-Poll-Frames findet zwischen zwei Phasen statt. Die erste ist die CFP (Contention-Free-Period-) Phase. Während dieser Phase versuchen andere Stationen nicht, auf das Medium zuzugreifen. Zugriff bekommt diejenige Station, welche das CF-Poll-Frame erhalten hat. Diese Phase wird entweder durch ein CF-End-Frame oder nach einer bestimmten Zeitspanne beendet. Danach folgt die zweite Phase. Diese wird CP-(Contention-Period-) Phase genannt. In dieser Phase erhält diejenige Station den Zugriff auf das Medium, welche entweder ein CF-Poll-Frame erhalten hat oder den kürzesten AIFS plus Backoff-Zeit hat.

DLS (DIRECT LINK SETUP)

Mit DLS wurde die Möglichkeit geschaffen, dass Stationen direkt untereinander kommunizieren. So müssen nicht alle Daten über den Access Point gesendet werden. Um eine DLS-Sitzung aufzubauen, sind folgende Schritte notwendig:

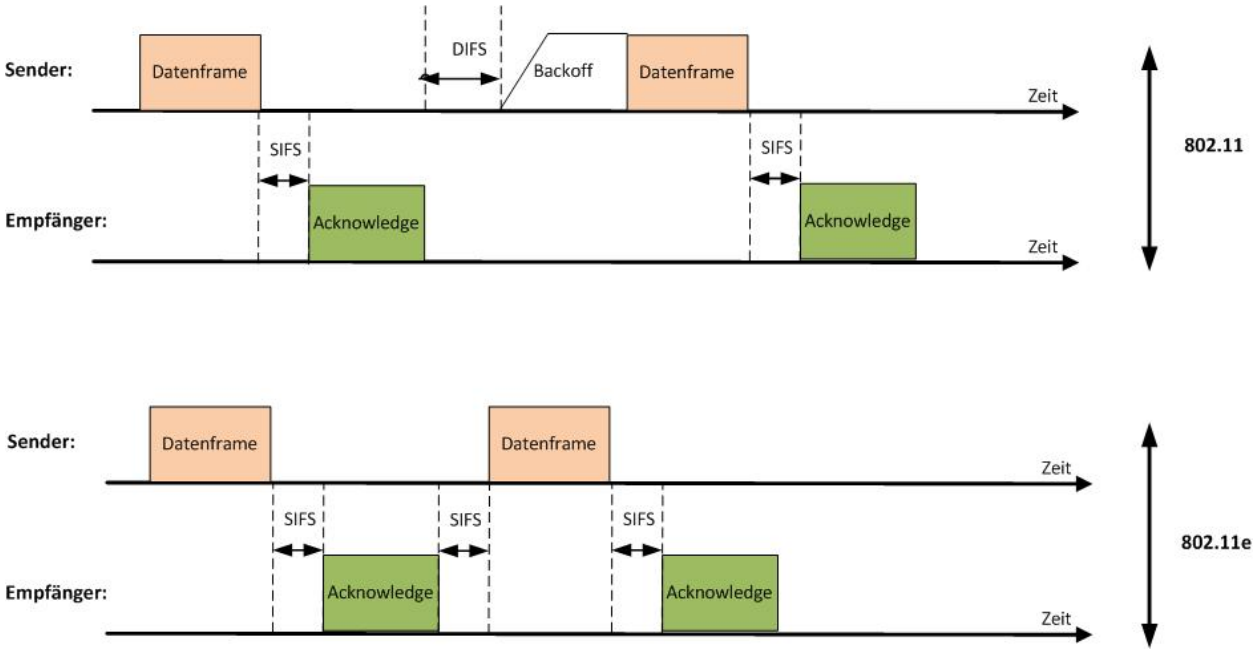
1. Eine Station, die DLS verwenden möchte, sendet einen DLS-Request an den Access Point.
2. Wenn der Access Point DLS unterstützt, sendet er den DLS-Request an die Station weiter, mit der die Sitzung aufgebaut werden soll. Falls er DLS nicht unterstützt, wird ein DLS-Response-Action-Frame mit dem Status „not allowed“ zurückgesendet.
3. Die Station sendet ein DLS-Response-Action-Frame zurück. Im Action-Frame ist der Status „Success“ enthalten. Success bedeutet, dass die Station es unterstützt und verwenden möchte.
4. Der Access Point sendet das DLS-Response-Frame an die initiierende Station weiter.
5. Nach dem Empfang des DLS-Response-Frames können Daten direkt zwischen den Stationen ausgetauscht werden.



Um die DLS-Sitzung wieder abzubauen, gibt es zwei Möglichkeiten. Die erste Möglichkeit ist, dass die Station, welche die Sitzung beenden will, ein DLS-Teardown-Frame sendet. Die zweite Methode beruht auf dem „inactivity Timer“. Sobald während einer bestimmten Zeitspanne keine Daten zwischen den Stationen ausgetauscht wurden, wird die Sitzung automatisch beendet.

BURSTING

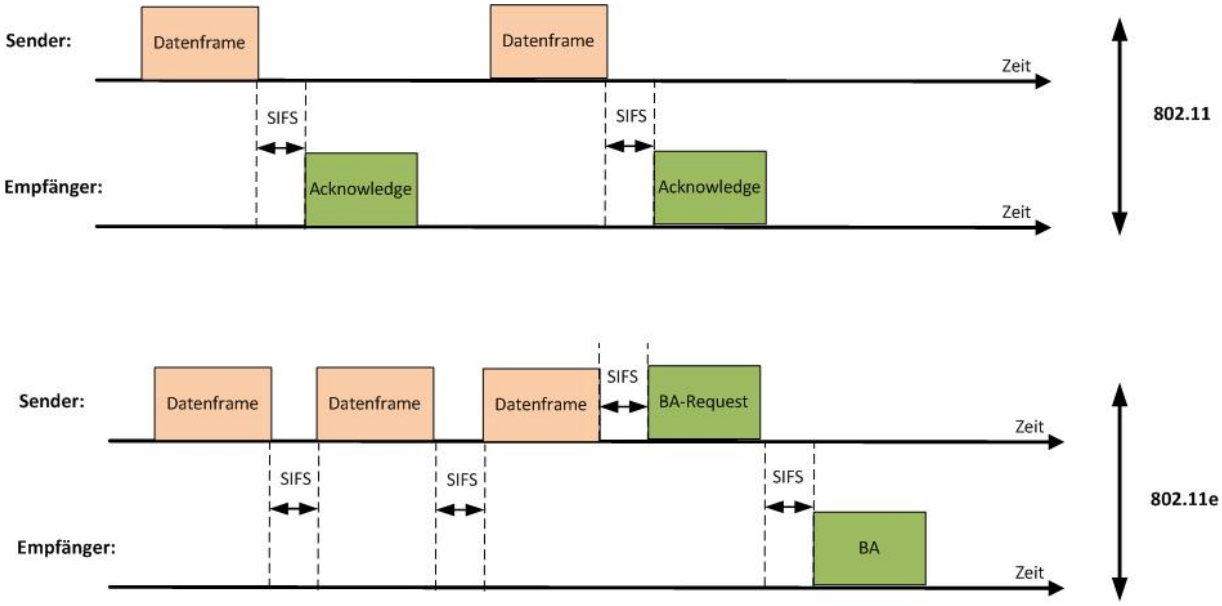
Eine weitere Verbesserung des Durchsatzes wurde durch das Bursting erreicht. Dabei darf eine Station so lange Daten übertragen, bis ihr TXOP-Limit erreicht wurde. Das TXOP-Limit ist im Beacon- und im Probe-Response-Frame enthalten. Dadurch erhält eine Station die Angabe einer Zeitdauer, während der sie Daten übertragen darf. Durch das Bursting ergibt sich eine Effizienzsteigerung beim Zugriff auf das Medium. Eine Station muss nach dem Erhalt eines ACK-Frames nicht wieder ein DIFS inkl. Backoff-Zeit abwarten, bevor sie ein Frame übertragen darf. Vielmehr kann sie nach einem SIFS sofort wieder auf das Medium zugreifen und das nächste Frame übertragen.



BLOCK-ACKNOWLEDGEMENT

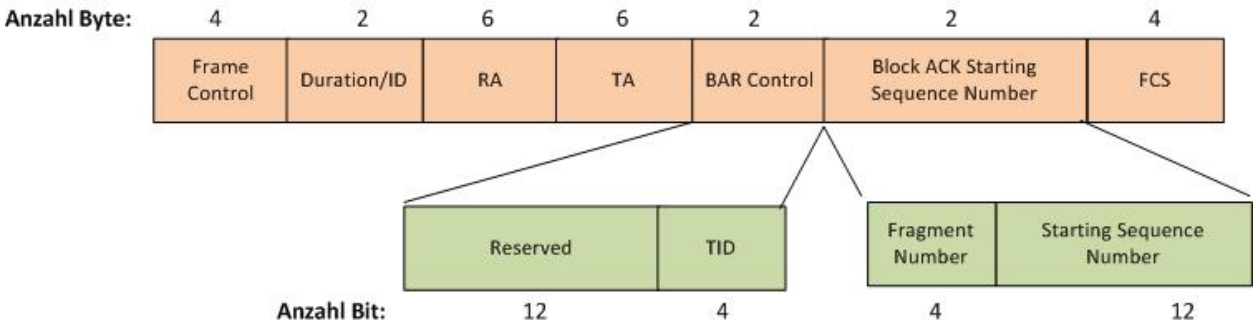
Beim gewöhnlichen WLAN wird jedes Unicast-Frame nach dem Empfang bestätigt. Dies ist allerdings nicht sehr performant. Aus diesem Grund wurde im 802.11e-Standard das Block-Acknowledgement eingeführt. Dieses erlaubt das Empfangen mehrerer Frames hintereinander, ohne dass jedes Frame einzeln bestätigt werden muss. Diese Methode erlaubt es, dass bis zu 64 MPDUs durch ein einzelnes Frame, das sogenannte Block-Acknowledgement-Frame, bestätigt werden. Dadurch wird der Overhead enorm reduziert, da für die Bestätigung lediglich noch ein Block-ACK-Frame benötigt wird. Ob dieser BA-Mechanismus verwendet werden kann, hängt von den Stationen ab. Zu Beginn der Übertragung sendet der Sender ein ADDBA-Request an den Empfänger. Wenn der Empfänger das Block-Acknowledgement unterstützt, sendet er ein ADDBA-Reply zurück. Dadurch erfahren die Stationen, ob die Übertragung mittels des BA-Mechanismus getätigt werden kann. Danach werden die Daten übertragen und der Sender sendet zum Schluss einen BA-Request mit. Der Empfänger bestätigt über das Block-ACK-Frame alle vom Sender erhaltenden Frames. Wenn die Übertragung abgeschlossen

ist, wird vom Sender ein DELBA-Frame gesendet. Dieses dient dazu, dem Empfänger zu signalisieren, dass die Station keine weiteren Daten mehr zu senden hat. Somit kann der Empfänger die ihm zugeteilten Ressourcen wie beispielsweise Empfangspuffer freigeben.



BA-REQUEST-FRAME-FORMAT

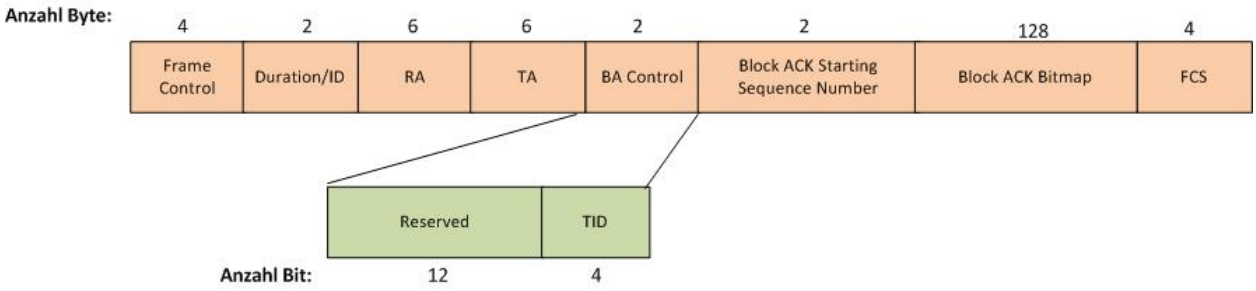
In der untenstehenden Abbildung ist der Aufbau eines BA-Request-Frames dargestellt.



Feld:	Wert:
Duration/ID	Ist die Dauer (in µs), die benötigt wird, um das BA-Frame zu senden, inklusive eines SIFS.
RA	Ist Empfängeradresse des BA-Request-Frames.
TA	Ist die Senderadresse des BA-Request-Frames.
BAR Control	Enthält die TID, für die der BA-Request gesendet wird.
Block ACK Starting Sequence Control	Die Starting Sequence Number enthält die Sequenznummer der ersten MSDU, für die der BA-Request gesendet worden ist. Bei der Fragmentnummer sind alle Bits auf 0 gesetzt.

BA-FRAME-FORMAT

In der folgenden Abbildung ist der Aufbau eines BA-Frames dargestellt.



Feld:	Beschreibung:
Duration/ID	Ist die Duration/ID vom BA-Request-Frame abzüglich der Zeit die benötigt wird, um das ACK-Frame zu senden, inkl. SIFS Intervall.
RA	Empfängeradresse des BA-Frames
TA	Senderadresse des BA-Frames
BA Control	Enthält die TID
Block ACK Starting Sequence Control	Dies ist der gleiche Wert wie im BA-Request-Frame. Der empfangene Wert wird in dieses Feld kopiert.
Block ACK Bitmap	Ist ein 128 Byte langes Feld und gibt an, welche MSDU/ MPDU erfolgreich empfangen wurde. Für jede MSDU/MPDU sind 2 Byte reserviert. Daher kann man maximal 64 MPDUs auf einmal bestätigen. Wenn für eine MPDU der Wert 1 vorhanden ist, so wurde die MPDU empfangen. Hingegen wurde die MPDU nicht empfangen, wenn im Feld ein Wert von 0 steht.

Im 802.11e-Standard werden zwei unterschiedliche Arten von Block-Acknowledgement unterschieden. Diese sind immediate BA und delayed BA.

Immediate BA

Beim immediate BA sendet die Station einen Burst an Daten, welche durch ein SIFS-Intervall getrennt sind. Am Ende der Übertragung sendet die Station ein BA-Request Frame. Sobald der Empfänger das BA-Request Frame empfängt, muss dieser das BA-Frame zurücksenden.

Delayed BA

Auch hier wird ein Burst an Daten gefolgt von einem BA-Request gesendet. Der Unterschied ist aber, dass der Empfang mittels eines normalen ACK-Frames bestätigt wird. Das eigentliche BA-Frame wird dann zu einem späteren Zeitpunkt gesendet.

NO-ACKNOWLEDGEMENT

Beim 802.11e-Standard hat eine Station die Möglichkeit, selber festzulegen, ob ihre Frames bestätigt werden müssen oder nicht. Dies ist vor allem bei echtzeitkritischen Daten wie VoIP oder Video der Fall. Wenn No-ACK verwendet wird, so wird im QoS Control Field das fünfte Bit auf 1 und das sechste Bit auf 0 gesetzt.

DER IEEE-802.11N-STANDARD

Beim 802.11n-Standard handelt es sich um den momentan neuesten Standard, welcher in WLANs eingesetzt wird. Die Brutto-Datenrate liegt bei 300–600 Mbps. Doch wieso ist dieser Standard so viel schneller als seine Vorgänger? Dazu wurden diverse verschiedene neue Mechanismen eingesetzt, welche im Folgenden beschrieben werden.

OFDM

Wie der 802.11g-Standard benutzt auch der 802.11n-Standard OFDM als Modulationstechnik. Im Unterschied zum 802.11g-Standard benutzt der 802.11n-Standard jedoch nicht nur ein einzelnes Trägersignal für die Datensignale. Vielmehr werden die Datensignale auf mehrere parallele Trägersignale moduliert. Dabei stehen im N-Standard neu 52 Trägersignale zur Verfügung.

MIMO

MIMO (Multiple Input Multiple Output) ist eine der wichtigsten Neuerungen im 802.11n-Standard. Durch MIMO hat eine Station oder ein Access Point mehrere Antennen zum Senden bzw. Empfangen zur Verfügung. Der Datenstrom wird dabei aufgeteilt und in Form verschiedener Datenströme übertragen. Bei der MIMO-Technologie wird ein Raummultiplex-Verfahren angewendet. Das heisst, dass auf der gleichen Frequenz mehrere Datenströme übertragen werden können, obwohl es ein shared medium ist. Dies ist deshalb möglich, weil jedes ausgesendete Signal im Raum anders reflektiert wird. Somit ist jeder einzelne Datenstrom charakterisierbar. Generell werden bei MIMO bis zu vier parallele Datenströme verwendet. Diese Datenströme werden „Spatial Streams“ genannt.

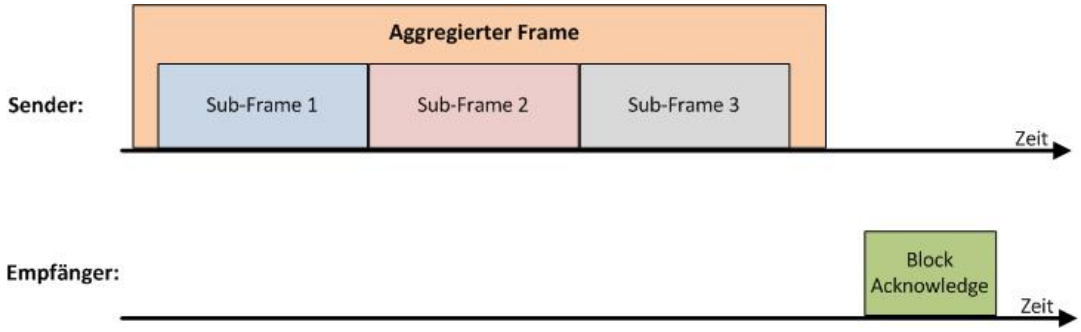
40-MHZ-KANÄLE

Beim 802.11n-Standard ist durch die Kanalbündelung von zwei 20-MHz-Kanälen die Erweiterung auf einen 40-MHz-Kanal möglich. Die Bündelung im N-Standard ist nur durch zwei direkt benachbarte Kanäle möglich. Aus diesem Grund ist die Bündelung der Kanäle nur im 5-GHz-Bereich erlaubt. Ein 40-MHz-Kanal hat den Vorteil, dass er mehr als doppelt so viele Trägerfrequenzen bietet wie ein 20-MHz-Kanal. Im 40-MHz-Kanalbereich stehen nämlich 108 Trägersignale zur Verfügung.

Um die Kompatibilität mit älteren Standards zu ermöglichen, muss der 40-MHz-Kanal logisch getrennt werden. Es besteht ja immer noch die Möglichkeit, dass im Netzwerk Stationen vorhanden sind, welche den 802.11n-Standard nicht implementiert haben. Diese sind somit auf 20-MHz-Kanäle beschränkt. Aus diesem Grund übernimmt der erste 20-MHz-Kanal die Funktion des Kontrollkanals. Hier werden beispielsweise Beacon-Frames, Probe-Requests, Probe-Responses etc. gesendet. Dadurch ist sichergestellt, dass auch Stationen Informationen über das Netzwerk erhalten, welche nur einen 20-MHz-Kanal unterstützen.

FRAME-AGGREGATION

Frame-Aggregation bezeichnet die Bündelung mehrerer einzelner Frames zu einem grossen Frame, bevor dieses übertragen wird. Somit ist pro aggregiertes Frame nur noch ein Physical-Layer-Header nötig. Die maximale Länge eines solchen Frames ist 65'535 Byte bzw. 64 MPDUs. Vom Prinzip her ist es mit den Jumbo-Frames im Ethernet identisch. Somit kann anstelle von vielen kurzen Frames, deren Empfang einzeln bestätigt werden muss, ein langes Frame gesendet werden. Zusätzlich muss bei der Übertragung zwischen zwei Frames ein IFS liegen. Dies ist bei der Frame-Aggregation nur am Anfang und am Ende der Fall. Zwischen den einzelnen Sub-Frames wird kein IFS angehängt. Der Overhead wird somit minimiert, vor allem wenn eine Station grosse Datenmengen zu übertragen hat.



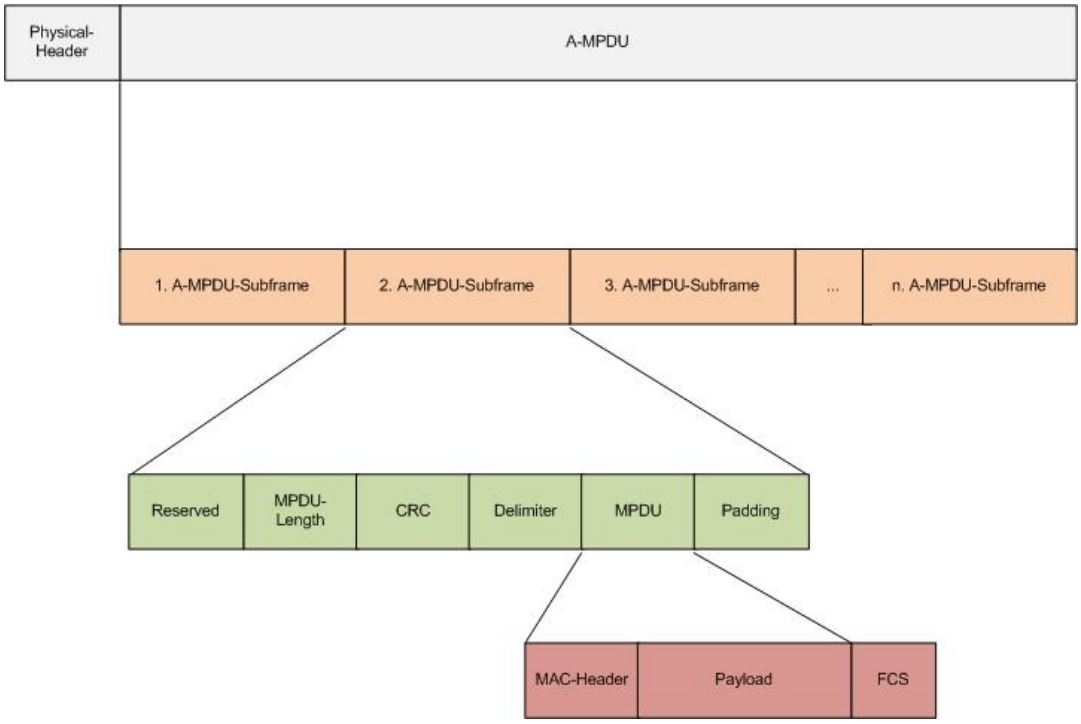
Es gibt zwei Arten der Frame-Aggregation. Zum Einen die sogenannte Aggregated MAC Service Data Unit (A-MSDU) und zum Anderen die Aggregated MAC Protocol Data Unit (A-MPDU). Der Unterschied zwischen den beiden liegt darin, wo im ISO/OSI-Referenzmodell aggregiert wird. Bei der A-MSDU wird oberhalb des MAC-Layers aggregiert. Dabei werden mehrere MSDUs zu einer MPDU zusammengefasst. Bei der A-MPDU wird unterhalb des MAC-Layers aggregiert. Somit werden mehrere MPDUs zu einer PSDU (Physical Service Data Unit) zusammengefasst.

Das Aggregation-Frame unterliegt aber auch Einschränkungen. Frames können nur aggregiert werden, wenn sie vom gleichen Sender zum gleichen Empfänger übertragen werden. Eine weitere Limitierung besteht darin, dass alle Frames, die aggregiert werden, bereits zum Senden bereit sein müssen. Andernfalls kann nicht aggregiert werden. Dies kann dazu führen, dass Frames verzögert übertragen werden, weil der Sender wartet, bis eine gewisse Anzahl Frames zum Senden bereit ist.

A-MPDU

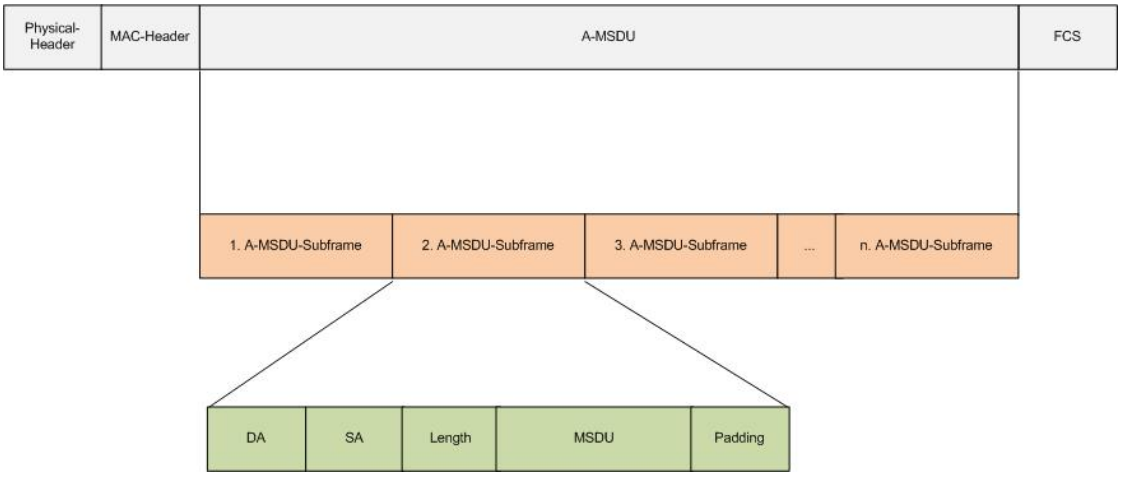
Hierbei werden mehrere Frames zu einer A-MPDU zusammengefasst und übertragen. Bei den MPDU-Subframes handelt es sich um komplette Frames inklusive MAC-Header, den Payload sowie eine Frame Check Sequence (FCS). Für die Bildung des A-MPDU-Subframes wird jedem Frame noch ein vier Byte langer Header hinzugefügt. Dieser besteht aus dem Feld Reserved, der MPDU-Länge, dem CRC sowie einem Delimiter. Dieser Header dient zur Abgrenzung der einzelnen Frames. Die maximale Länge eines Subframes beträgt 4095 Bytes. Die Gesamtlänge einer aggregierten MPDU ist

auf 65’535 Byte beschränkt. Zusätzlich gibt es für jede MPDU noch ein Padding. Dies aufgrund der Tatsache, dass ein Subframe immer ein Vielfaches von 4 Byte lang sein muss.



A-MSDU

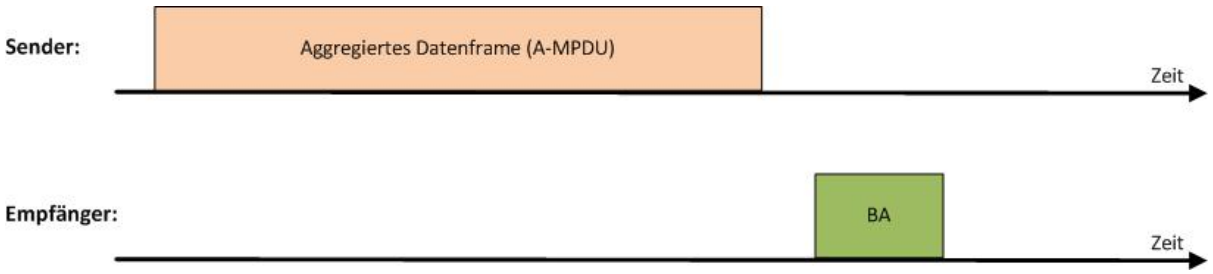
Bei der Aggregation der MSDUs werden mehrere MSDU-Subframes zu einem Frame zusammengefasst. Jedes MSDU-Subframe besteht aus einem Header, der MSDU sowie dem Padding. Der wesentliche Vorteil dieser Art der Aggregation ist, dass hier nur ein MAC-Header und eine FCS hinzugefügt werden müssen. Somit verringert sich der Overhead im Gegensatz zur A-MPDU. Jedoch ergibt sich daraus auch ein Nachteil. Weil nur eine FCS vorhanden ist, muss bei einem Fehler das komplette aggregierte Frame nochmals übertragen werden.



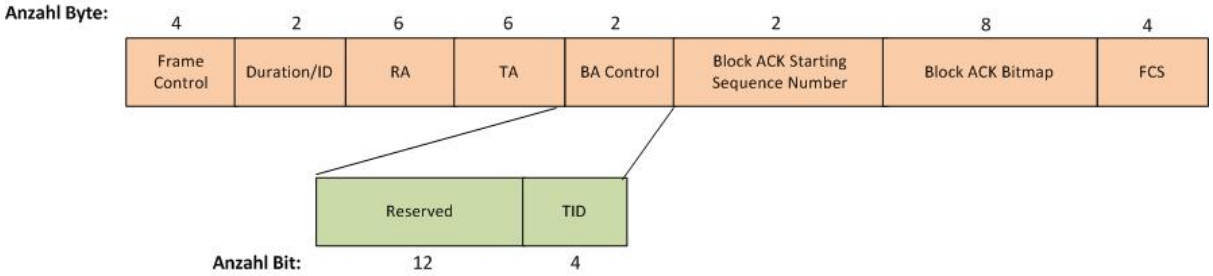
BLOCK-ACKNOWLEDGEMENT

Das Block-Acknowledgement wurde für den 802.11n-Standard noch einmal abgeändert und verbessert.

Die erste Verbesserung wurde im impliziten Block-ACK vorgenommen. Dabei wird auf den BAR (Block Acknowledge Request) verzichtet und es wird nur noch das BA (Block Acknowledge) zurückgesendet, um die aggregierten Frames zu bestätigen. Wenn ein aggregiertes MPDU übertragen wird, müssen alle MPDUs bestätigt werden. Dabei enthält das BA-Frame ein Block-ACK-Bitmap-Feld. Dieses Feld ist 128 Byte lang. Darin wird der Empfang jeder MPDU dargestellt. Ist der Inhalt für eine MPDU 1, dann wurde die betreffende MPDU erfolgreich empfangen. Ist der Inhalt dagegen 0, so wurde die MPDU nicht empfangen und muss zu einem späteren Zeitpunkt erneut übertragen werden.

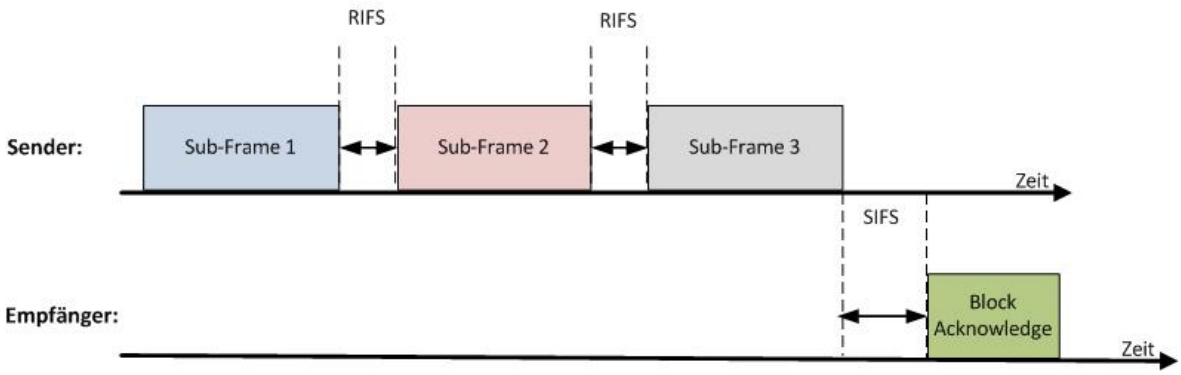


Eine weitere Optimierung ist die Kompression des BA-Frames. Anstelle von 128 Byte, die benötigt werden, um ein aggregiertes Frame zu bestätigen, wurde das BA-Frame komprimiert. Nun wird für jede MPDU, die bestätigt werden muss, nur noch ein Bit verwendet. Weil in einem aggregierten MPDU-Frame maximal 64 Subframes enthalten sein können, benötigt man für die Bestätigung lediglich 64 Bit. Dadurch wird der Overhead von 128 Byte auf acht Byte verringert.



RIFS

Wie im Kapitel zu IFS erklärt wurde, wird zwischen zwei auszusendenden Frames immer eine Pause eingelegt. Je nach verwendetem Frame-Typ ist dieser Abstand unterschiedlich lang. Zur weiteren Steigerung des Durchsatzes wurde ein weiterer IFS-Typ definiert. Dieser Typ wird als Reduced Inter Frame Space bezeichnet und hat eine Dauer von zwei µs. RIFS wird verwendet, wenn ein Frame nicht aggregiert werden kann, aber ein Burst an Daten gesendet wird. Wenn nun Station A an Station B mehrere Frames hintereinander sendet, dann muss zwischen den einzelnen Frames nicht ein ganzer SIFS abgewartet werden, bis das nächste Frame gesendet werden darf. Das nächste zu sendende Frame kann nach Ablauf eines RIFS sofort ausgesendet werden. Dies beschleunigt den Zugriff auf das Übertragungsmedium, was einen positiven Einfluss auf die Datenrate hat.



PHY-PARAMETER

In der folgenden Tabelle sind die verschiedenen physikalischen Parameter des 802.11n-Standards aufgelistet:

Parameter	Wert
SlotTime:	20 µs (gemischter Modus im 2.4-GHz-Frequenzband) 9 µs (im 2.4-GHz-Frequenzband, nur 802.11n-Stationen) 9 µs (im 5-GHz-Frequenzband, nur 802.11n-Stationen)
SIFSTime:	10 µs (im 2.4-GHz-Frequenzband) 16 µs (im 5-GHz-Frequenzband)
PIFSTime:	30 µs (im 2.4-GHz-Frequenzband und gemischter Modus) 19 µs (im-2.4 GHz-Frequenzband und nur 802.11n-Stationen) 25 µs (im 5-GHz-Frequenzband)
DIFSTime:	50 µs (gemischter Modus im 2.4-GHz-Frequenzband) 28 µs (im 2.4-GHz-Frequenzband, nur 802.11n-Stationen) 34 µs (im 5 GHz Frequenzband, nur 802.11n-Stationen)
RIFSTime:	2 µs
Präambel-Dauer:	16 µs
Dauer für Physical-Layer-Header:	4 µs
CWmin:	15
CWmax:	1023
Maximale MPDU-Länge:	65’535 Byte

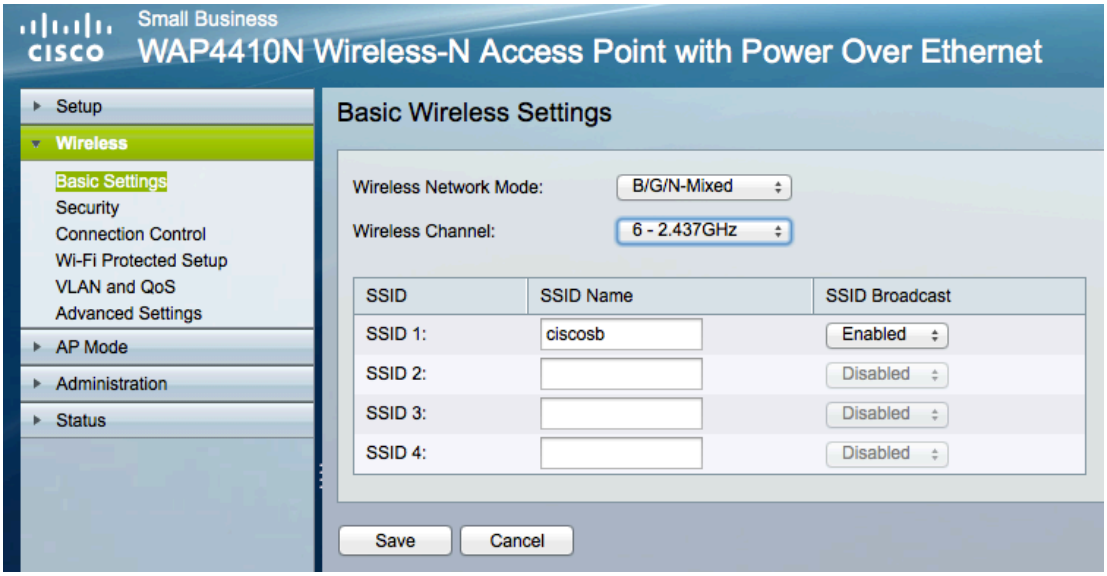
MESS-HARDWARE

ACCESS POINTS

CISCO WAP4410N

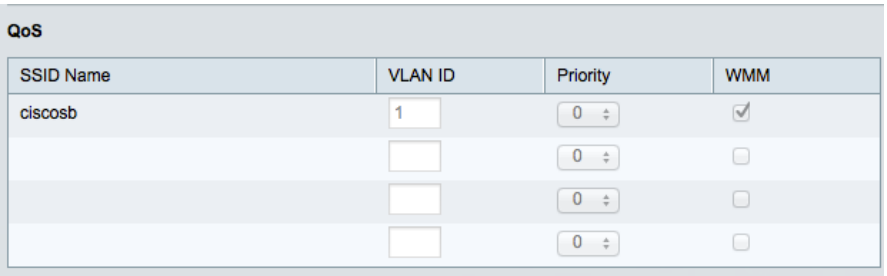
Beim Cisco Access Point handelt es sich um einen Wireless-N-Standard-Access-Point, welcher auch mit den älteren Standards kompatibel ist. Dieser Access Point unterstützt nur den 2.4-GHz-Frequenzbereich. Im Weiteren werden nur die für diese Arbeit relevanten Funktionen des Access Points beschrieben. Auf die Verschlüsselung wird hier nicht eingegangen, da die Messungen im Rahmen dieser Arbeit ausschliesslich unverschlüsselt erfolgten.

BASIC SETTINGS



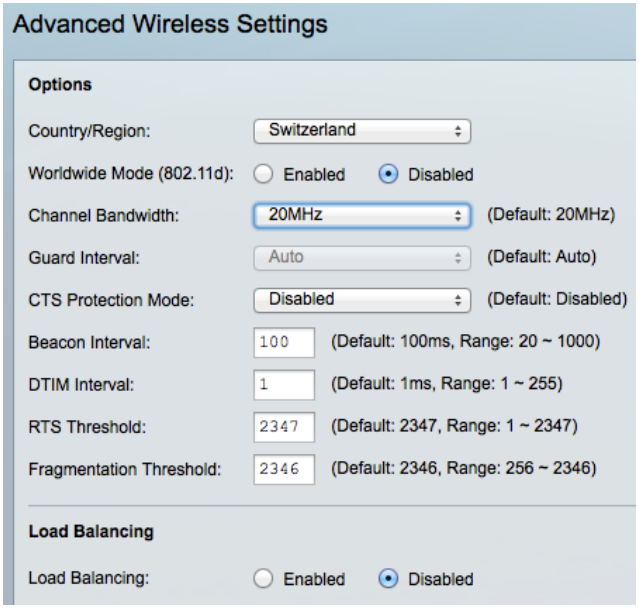
Einstellung	Werte	Beschreibung
Wireless Network Mode	• B-Only • G-Only • N-Only • B/G-Mixed • B/G/B-Mixed	Hier kann der entsprechende Modus ausgewählt werden.
Wireless Channel	Kanäle 1–13 im 2.4-GHz-Bereich	Hier kann der zu verwendende 20-MHz-Kanal bzw. die Frequenz ausgewählt werden, welche vom WLAN benutzt werden soll. Wichtig ist, dass man einen Kanal auswählt, der nicht von mehreren WLANs verwendet wird. Ansonsten läuft man Gefahr, dass Interferenzen entstehen und diese sich negativ auf die Geschwindigkeit auswirken.
SSID	SSID 1–4	Dies ist der Name der BSS oder EBSS. Es werden bis zu vier verschiedene SSIDs unterstützt.

QOS



Einstellung	Werte	Beschreibung
SSID Name	• variabel	Name des WLAN
VLAN ID	• 1–255	Angabe des VLAN, welches für die SSID verwendet wird
Priority	• 0-7	Setzen der Priorität für eine SSID. 0 ist dabei die höchste und 7 die niedrigste Priorität
WMM	• aktiviert/deaktiviert	Aktivieren bzw. Deaktivieren des WMM

ADVANCED WIRELESS SETTINGS



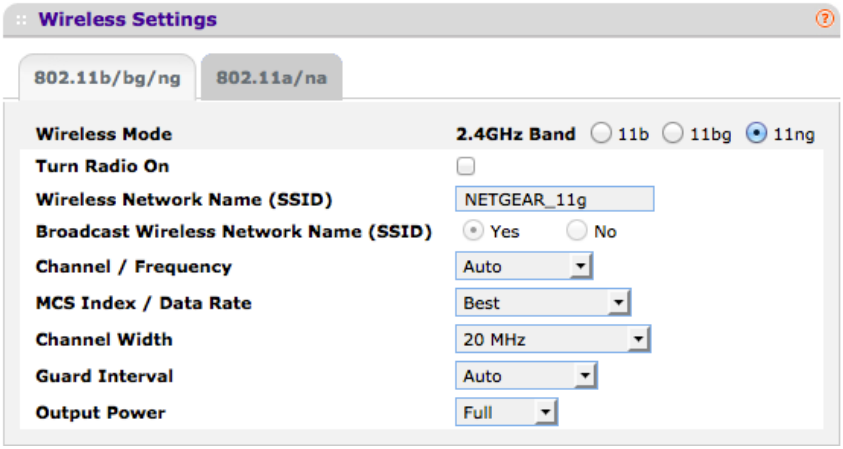
Einstellung	Werte	Beschreibung
Country / Region	• Switzerland • Spain • etc.	Hier sind die Länder aufgelistet, für die der Access Point vorgesehen ist. Da beim Access Point 13 Kanäle verwendet werden dürfen, sind z.B. die USA nicht aufgelistet, da man dort lediglich 11 Kanäle verwenden darf.
Worldwide Mode	• Enable	Erlaubt das Aktivieren von 802.11d. Auch hier gehört die Regelung der Kanäle in verschiedenen

	• Disable	Ländern / Regionen dazu.
Channel Bandwidth	• 20 MHz • 40 MHz	Auswahl der Kanalbreite. Wenn es auf 40 MHz gesetzt ist, wird der 40-MHz-Kanal nur von N-Standard-Stationen verwendet. 802.11g- und 802.11b-Stationen benutzen dann immer noch den 20-MHz-Kanal.
Guard Interval	• 400 ns • 800 ns	Manuelles Einstellen der Guard-Intervalle im N-Standard. Dabei handelt es sich um die Zeit, die nach dem Senden eines OFDM-Symbols bis zum nächsten abgewartet werden muss. Beim N-Standard wird 400 ns und bei B/G-Standard 800 ns verwendet.
CTS Protection Mode	• Auto • Disable	CTS-Verwendung deaktivieren oder auf Auto stellen. Dadurch wird sichergestellt, dass 802.11b-Stationen Zugriff auf das WLAN haben, auch wenn sehr viele G- oder N-Stationen vorhanden sind.
Beacon Interval	• 20–1000 ms	Gibt an, in welchen Zeitabständen der Access Point die Beacon-Frames aussendet.
DTIM Interval	• 1–250 ms	Gibt das DTIM-Intervall an. Clients werden darüber informiert, dass der Access Point Broadcast- / Multicast-Daten für den Client hat. Nach Ablauf des DTIM sendet der Access Point diese Daten an die Clients.
RTS Treshhold	• 1–2347 Byte	Gibt an, ab welcher Frame-Länge der RTS-/CTS-Mechanismus aktiviert wird.
Fragmentation Threshold	• 256–2346 Byte	Angabe der maximalen Länge des Pakets, bevor das Paket fragmentiert wird.
Load Balancing	• Enable • Disable	Hier kann pro SSID ein Utilization Treshhold in Prozent angegeben werden. Wird dieser Prozentsatz erreicht, wird den Stationen verweigert, sich mit dem Access Point zu assoziieren.

NETGEAR WNDAP350

Der Netgear Access Point unterstützt den 2.4-GHz- und den 5-GHz-Bereich. Auch hier werden nur diejenigen Funktionen beschrieben, welche für diese Arbeit relevant sind.

BASIC WLAN SETTINGS 2.4 GHZ

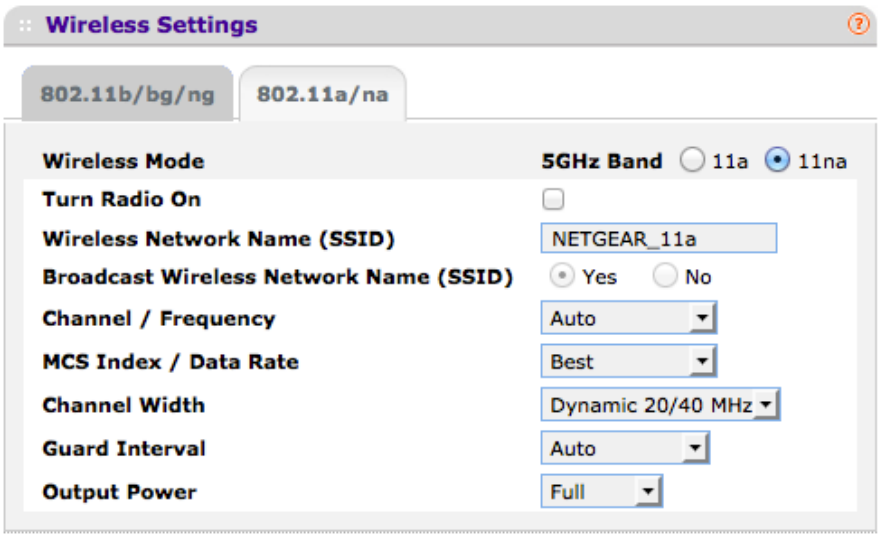


Einstellung	Werte	Beschreibung
Wireless Mode	• 11b • 11bg • 11ng	Bei 11b werden nur 802.11b-Stationen unterstützt. Beim 11bg werden sowohl 802.11b- als auch 802.11g-Stationen unterstützt. Bei 11ng werden alle Stationen (B, G,N) unterstützt.
Wireless Network Name	variabel	Dies ist der Name des WLAN.
Broadcast Wireless Network Name	• Yes • No	Gibt an, ob der Name der SSID in den Beacon-Frames mitgesendet werden soll oder nicht. Dadurch ist es möglich, dass das WLAN nicht automatisch durch das Betriebssystem aufgefunden wird.
Channel / Frequency	• Auto • Kanäle 1 - 13	Mittels der „Auto-Funktion“ sucht sich der Access Point jenen Kanal aus, welcher die geringsten Interferenzen aufweist. Trotzdem ist es auch möglich, den gewünschten Kanal manuell einzustellen.
MCS Index / Data Rate	• Best • Index mit Datenrate	Hier kann die Datenrate angegeben werden. Bei Best wird die schnellste unterstützte Datenrate verwendet. Die Datenrate ist von der Kanalbreite und dem Guard-Intervall abhängig. Bei 20 MHz sind unter Verwendung des Short-Guard-Intervalls (400ns) Bruttodatenraten bis 144.44 Mbps möglich. Beim Long-Guard-Intervall (800ns) sind Bruttodatenraten bis 130 Mbps möglich. Bei 40 MHz sind unter Verwendung des Short-Guard-Intervalls Bruttodatenraten bis 300 Mbps möglich. Mit

		Long-Guard-Intervall sind Bruttodatenraten bis 270 Mbps möglich.
Channel Width	• 20 MHz • 40 MHz • Dynamic 20/40 MHz	Auswahl der Kanalbreite.
Guard Interval	• Auto • Long	Bei Auto wird versucht, das Short-Guard-Intervall zu verwenden (400ns). Wenn dies nicht klappt, wird das Long Guard verwendet. Des Weiteren kann man das Guard-Intervall manuell auf Long (800ns) setzen. Somit wird zwischen einzelnen OFDM-Symbolen eine Pause von 800ns eingelegt.
Output Power	• Full • Half • Quarter • Eighth • Minimum	Einstellen der Signalstärke. Dabei wird von einem Schritt zum anderen die Signalstärke um die Hälfte verringert. Dies entspricht einer Dämpfung von 3db.

BASIC WLAN SETTINGS 5 GHZ

Hier sind dieselben Einstellungsmöglichkeiten wie im 2.4-GHz-Bereich vorhanden. Die einzigen Unterschiede sind der Wireless-Modus und die 5-GHz-Kanäle.

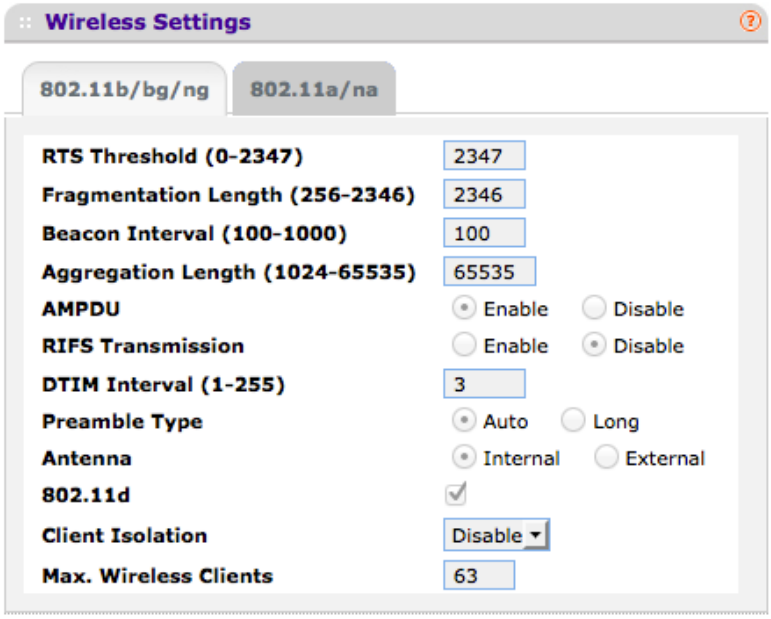


Einstellung	Werte	Beschreibung
Wireless Mode	• 11a • 11na	Bei 11a können nur 802.11a-fähige Stationen verwendet werden. Bei 11na können 802.11a- wie auch 802.11n-Stationen auf dem 5-GHz-Band benutzt werden.
Channel / Frequency	• Auto • Kanäle 36–136	Auswahl des Kanals oder Auto, um den Kanal automatisch auszuwählen.

BASIC QOS SETTINGS

Hier können für alle Standards und Frequenzbereiche QoS nach dem 802.11e-Standard aktiviert werden. Dadurch wird die Priorisierung von Daten ermöglicht. Ist WMM nicht aktiviert, können auch die erweiterten QoS-Parameter nicht konfiguriert werden.

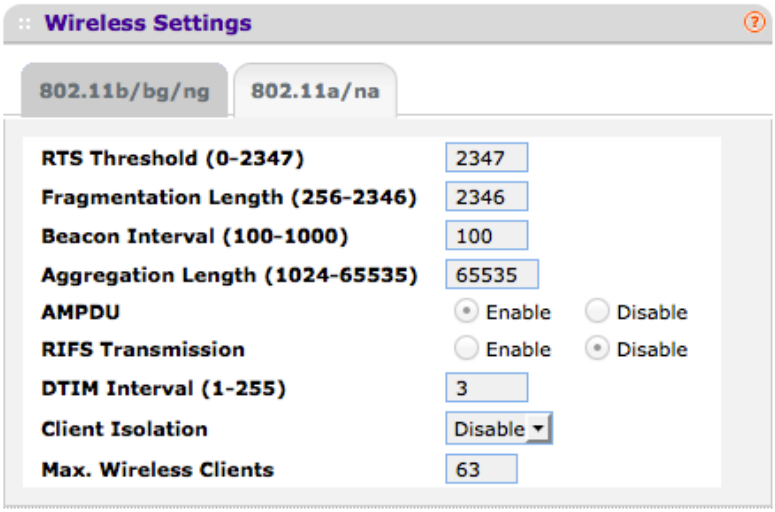
ADVANCED WIRELESS SETTINGS 2.4 GHZ



Einstellung	Werte	Beschreibung
RTS Threshold	• 0–2347 Byte	Gibt die Frame-Länge an, ab welcher das RTS-Verfahren verwendet werden soll. Da ein einzelnes Frame nie länger sein kann als 2346 Byte, ist beim Wert 2347 der RTS-/CTS-Mechanismus deaktiviert.
Fragmentation Length	• 256–2346 Byte	Pakete, die die hier angegebene Länge übersteigen, werden fragmentiert.
Beacon Interval	• 100–1000 ms	Zeitintervall zwischen dem Aussenden von zwei Beacon-Frames.
Aggregation Length	• 1024–65’535 Byte	Maximale Länge eines aggregierten Frames.
AMPDU	• Enable • Disable	Ermöglicht die Aggregation von Frames.

RIFS Transmission	• Enable • Disable	Aktivieren von RIFS für 802.11n-Stationen.
DTIM Interval	• 1–255	Angabe, nach wievielen Beacon-Frames ein DTIM an die Station gesendet wird.
Preamble Type	• Auto • Long	Ist auf Auto und verwendet normalerweise die Short Preamble. Sind jedoch noch 802.11b- und 802.11g-Stationen vorhanden, kann die Long Preamble konfiguriert werden.
Antenna	• Internal • External	Bei diesem Modell könnten noch externe Antennen angeschlossen werden. Hier kann ausgewählt werden, welche Antenne man verwenden möchte.
802.11d	• Enable • Disable	Erlaubt das Aktivieren von 802.11d. Dazu gehört die Regelung der Kanäle in verschiedenen Ländern / Regionen.

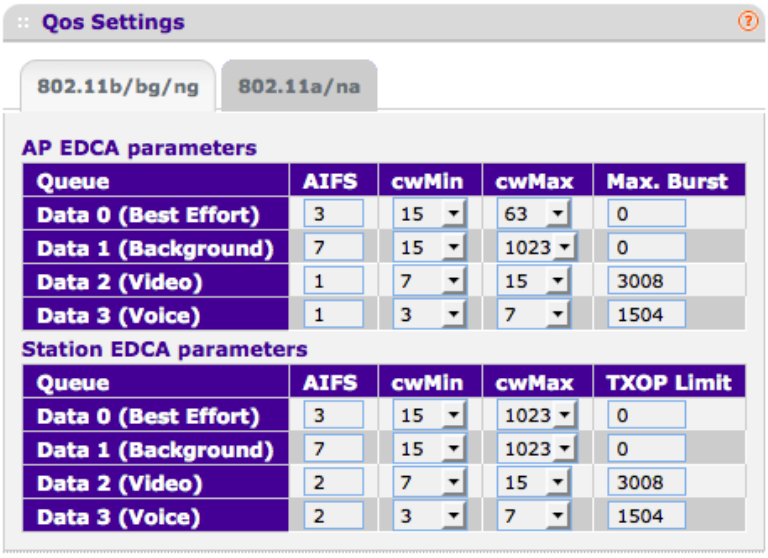
ADVANCED WIRELESS SETTINGS 5 GHZ



Wie zu erkennen ist, sind hier praktisch die gleichen Einstellungsmöglichkeiten vorhanden wie im 2.4-GHz-Band. Deshalb werden hier nur die Besonderheiten beschrieben. Im 5-GHz-Bereich wird ausschliesslich die Short Preamble verwendet. Aus diesem Grund kann dies nicht mehr eingestellt werden. Des Weiteren ist es nicht möglich, den 802.11d-Standard zu aktivieren. Der letzte Unterschied ist, dass es nur möglich ist, eine 2.4-GHz- externe Antenne an den Access Point anzuschliessen. Deshalb kann hier auch nicht die entsprechende Antenne ausgewählt werden.

ADVANCED QOS SETTINGS

Die QoS-Settings sind für den 2.4-GHz- und den 5-GHz-Bereich identisch. Deshalb werden sie nur einmal beschrieben.



Es werden zwei QoS Optionen unterschieden:

AP EDCA parameters:
definieren die EDCA-Parameter für verschiedene Formen von Verkehr, der vom Access Point an die Stationen gesendet wird.

Station EDCA parameters:
Definieren die EDCA-Parameter für Verkehr, der von den Stationen an den Access Point gesendet wird.

Queue-Einstellung	Beschreibung
Best Effort	Keine Priorisierung der Daten. Dabei handelt es sich meistens um normalen IP-Datenverkehr wie beispielsweise Internetverkehr etc.
Background	Geringste Priorität. Hier handelt es sich um nicht zeitkritische Daten.
Video	Die Übertragung von Videos erhält die zweithöchste Priorität. Auch hier resultiert eine geringe Verzögerung der Frames.
Voice	Dieser Verkehr erhält die höchste Priorität. Deshalb haben solche Frames die geringste Verzögerung. Zu den Daten gehören jene von VoIP- und anderen Streaming-Medien.
AIFS	Angabe in Sekunden, wi lange gewartet werden muss, bis Daten gesendet werden dürfen. Höher priorisierte Queues haben einen niedrigeren AIFS-Wert als andere und erhalten somit schneller Zugriff auf das Medium.
CWmin	Für jede Queue kann ein CWmin eingestellt werden, der für die Berechnung der Backoff-Zeit mit eingerechnet wird.
CWmax	Des Weiteren kann ein CWmax-Wert angegeben werden, der das obere Limit der Berechnung der Backoff-Zeit angibt.
Max. Burst Length	Definiert die Zeitdauer in ms, welche für die Übertragung eines Bursts erlaubt ist.

NOTEBOOKS

Für die Durchführung der Messungen stehen zwei Notebooks zur Verfügung. Auf diesen Notebooks ist das Linux-Betriebssystem BackTrack 5 installiert worden. BackTrack ist eine Linux-Distribution, mit der normalerweise die Sicherheit von Netzwerken überprüft wird. Es eignet sich aber auch für die Messung von Geschwindigkeiten im Netzwerk, da im Vergleich zu anderen Distributionen hier wenig Services installiert sind, welche im Hintergrund laufen und auf das Netzwerk zugreifen. Ein weiterer Vorteil ist, dass für die Messung benötigte Programme bereits auf der Distribution mitinstalliert sind. Als Beispiel sei hier Wireshark erwähnt.

Im Weiteren sind die Notebooks und deren Einstellungen genauer erläutert.

- Fujitsu Life Book S6420
  - CPU:
    - Core 2 Duo 2.8 GHz
  - RAM:
    - 4096 MB
  - WLAN-Netzwerkkarte mit drei Antennen
    - IP-Adresse: 192.168.1.10
    - Subnetzmaske: 255.255.255.0
    - MTU: 1500 Byte
  - Hostname: Notebook 1

- Fujitsu Celsius H250
  - CPU:
    - Core 2 Duo 2.2 GHz
  - RAM:
    - 2048 MB
  - Ethernet-Netzwerkkarte
    - IP-Adresse: 192.168.1.11
    - Subnetzmaske: 255.255.255.0
    - MTU: 1500 Byte
  - Hostname: Notebook 2

AIRPCAP NX USB-ADAPTER

Der AirPCAP NX ist ein USB-Adapter, der es ermöglicht, mit dem Wireshark-Programm die über die Luftschnittstelle übertragenen Daten aufzuzeichnen. Dieser Adapter wird für die Messungen benutzt, um die 802.11-Frames bei der Übertragung auf der Luftschnittstelle aufzuzeichnen und analysieren zu können. Dieser Adapter ist mit den Standards 802.11a/b/g/n kompatibel.

MESS-SOFTWARE

IPERF

IPerf ist ein Programm zur Messung der Bandbreite innerhalb eines Netzwerks. Um eine Messung durchführen zu können, benötigt man zwei Computer bzw. Notebooks, auf denen IPerf installiert ist. Dieses Programm ist frei erhältlich und kann auf Mac, Windows und Linux installiert werden. IPerf ist ein Client-Server-Programm und misst dabei den Durchsatz zwischen Client und Server. Der Vorteil von IPerf ist, dass es einfach über die Kommandozeile bedienbar/konfigurierbar ist. Für eine Messung werden immer ein Server und ein Client benötigt. Der Client ist dafür zuständig, die Messung zu starten und die zu übertragenden Daten an den Server zu übertragen. Beim Client kann die Bandbreite in bps angegeben werden, mit der er die Daten übertragen soll. Daraus ergibt sich eine konstante Bitrate, mit der Daten übertragen werden. Die Aufgabe des Servers ist es, die Daten zu empfangen, zu bestätigen und aufzuzeichnen. IPerf unterstützt auf dem Transport-Layer die Verwendung sowohl von TCP als auch von UDP. Welches Protokoll bei der Messung verwendet werden soll, ist einstellbar. Durch die Verwendung des UDP-Protokolls wird auf dem Server der Jitter wie auch der Verlust von Datengrammen angezeigt. Dadurch ist auch der Verlust von Datengrammen/IP-Paketen ersichtlich.

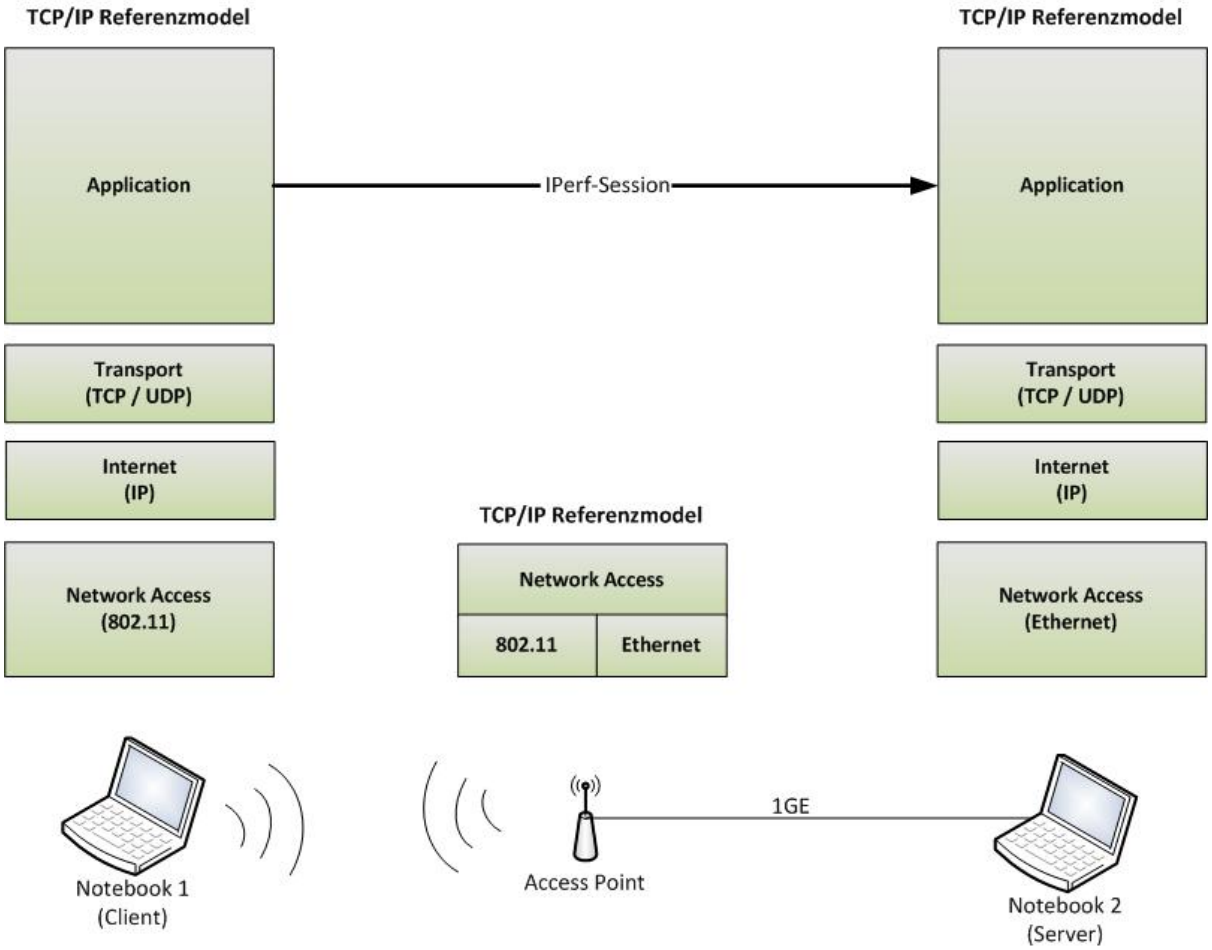
Um eine IPerf-Messung zu starten, müssen der Server und der Client gestartet werden. Um den Server zu starten, muss das Kommando „iperf –s“ in einer Shell angegeben werden. Der Client wird mit dem Kommando „iperf –c IP_DES_SERVERS“ gestartet. Zusätzlich können noch verschiedene Optionen als Argumente mit angegeben werden. Die für diese Arbeit wichtigsten Optionen sind in der untenstehenden Tabelle aufgelistet.

Option	Beschreibung
-p	Gibt den Port auf dem Client/Server an, auf dem eine Verbindung erwartet wird.
-u	Anstelle von TCP wird UDP verwendet.
-b	Angabe der Bandbreite in Bit pro Sekunde. Ist nur bei der Verwendung von UDP notwendig.
-t	Gibt die Dauer der Messung in Sekunden an.
-P	Hier kann man mehrere Clients simulieren. Dabei wird für jeden Client ein eigener Stream von Daten gesendet.
-l	Gibt die Länge der Daten in Byte an. Bei den Messungen wird hier eine Länge von 1472 Byte angegeben. Damit wird durch Hinzufügen des UDP- (8 Byte) und IP-Headers (20 Byte) die maximale MTU von 1500 Byte vollständig ausgenutzt.

MESSAUFBAU

Für die Durchführung der Messungen wird der unten dargestellte Messaufbau verwendet. Für die End-zu-End-Messung werden zwei Notebooks eingesetzt. Diese Notebooks sind jeweils mit dem Access Point verbunden und bilden somit ein Subnetz. Dabei ist das Notebook 1 mit dem Access Point über WLAN assoziiert. Das Notebook 2 ist via ein RJ45-Ethernet-Kabel mit dem Access Point verbunden. Der Access Point muss eine Medienkonvertierung von 802.11 nach Ethernet und umgekehrt durchführen.

Für die Messungen wird als Referenzmodell das TCP/IP-Modell verwendet. Durch die verschiedenen Layers ergibt sich die Möglichkeit, die Performance auf den verschiedenen Schichten zu analysieren. In dieser Arbeit geht es vor allem darum, die Performance des Network-Access-Layers in Bezug auf den 802.11-Standard zu analysieren. Dazu werden verschiedene Messszenarien erarbeitet, mit denen die Auswirkung der Performance analysiert wird. Dazu gehören beispielsweise die Optimierung von Management- und Kontroll-Frames sowie die Verwendung von Erweiterungen der implementierten Standards.



Auf dem Application-Layer wird für die Generierung von Frames das Tool IPerf verwendet. Dazu wird beim Client die Bitrate pro Sekunde angeben, mit der die Daten zum Server gesendet werden sollen. Im verwendeten Setup ist das Notebook 1 der IPerf-Client und das Notebook 2 der IPerf-Server.

Um die Performance messen zu können, wird auf dem Transport-Layer das UDP-Protokoll verwendet. Dieses Protokoll ist verbindungslos und kann deshalb nicht gewährleisten, dass alle gesendeten Frames beim Empfänger korrekt empfangen worden sind. Trotzdem eignet es sich für die Messung der Performance im Netzwerk. Dies aus dem Grund, dass im Gegensatz zu TCP kein Sliding-Window und Slow-Start für die Flusskontrolle verwendet wird. Daher kann ein Client unmittelbar mit der Übertragung der Daten bei voller Geschwindigkeit beginnen. Ein weiterer Vorteil ist, dass der Overhead von UDP geringer ist als derjenige von TCP. UDP fügt den einzelnen Segmenten einen Header von 8 Byte Länge an. Bei TCP hingegen wird jedem Segment ein Header mit 20 Byte Länge angehängt. Die Geschwindigkeit ist von verschiedenen Faktoren abhängig, beispielsweise von der Puffergrösse des Senders und Empfängers, der Bearbeitungszeit beim Sender, dem Empfänger und dem Access Point, der maximalen Übertragungsrate des verwendeten Mediums sowie der Laufzeit und der Round Trip Time des Signals.

Auf dem Internet-Layer wird zur Übertragung der Pakete das IP-Protokoll eingesetzt. Dieses ist verbindungslos und unzuverlässig. Das bedeutet, dass auch hier nicht gewährleistet ist, dass alle gesendeten Pakete beim Empfänger ankommen. Zusätzlich kann durch die Verwendung von IP nicht gewährleistet werden, dass die einzelnen Pakete ankommen und dass sie dies zu einer bestimmten Zeit tun. Dies liegt daran, dass IP weder eine Flusskontrolle noch einen Bestätigungsmechanismus einsetzt. Ob verlorene Pakete neu angefordert werden, hängt jeweils von der Applikation bzw. dem verwendeten Transport-Protokoll ab.

Beim Network-Access-Layer wird zwischen dem Notebook 1 und dem Access Point der 802.11-Standard eingesetzt. Da es in dieser Arbeit um die Performance von WLANs geht, liegt der Schwerpunkt der Messungen in der Übertragung zwischen diesen beiden Geräten. Dabei werden gewisse Funktionen auf dem Access Point aktiviert bzw. deaktiviert, um herauszufinden, welchen Einfluss eine Funktion auf die Performance im WLAN hat. Damit die Messungen transparent sind, wird die Verarbeitungszeit der einzelnen verwendeten Geräte gemessen. Dazu wird das ICMP-Protokoll verwendet. Somit wird die Verarbeitungszeit gemessen, welche durch den implementierten Protokoll-Stack der verschiedenen Komponenten zu Stande kommt. Zusätzlich wird die Laufzeit des Signals zwischen Notebook 1 und Notebook 2 gemessen. Auch dazu wird das ICMP-Protokoll verwendet. Der Access Point enthält einen integrierten Layer-2-Switch, welcher den Access Point mit dem Notebook 2 über GigabitEthernet verbindet. Dieses Setup ermöglicht eine End-zu-End-Kommunikation zwischen Notebook 1 und Notebook 2 über einen Access Point, wobei sowohl WLAN als auch Ethernet eingesetzt wird. Somit stören sich die beiden Notebooks untereinander nicht, da sie andere Layer-2-Protokolle verwenden. Wären beide Notebooks über WLAN mit dem Access Point assoziiert, so würden allein schon dadurch die Messresultate zur Performance des WLAN verzerrt, da sich die Notebooks untereinander bereits stören könnten.

MESSUNG DER ROUND TRIP TIME

Die Round Trip Time (RTT) ist die Zeitdauer, welche ein Paket benötigt, um vom Sender zum Empfänger hin und zurück übertragen zu werden. Ein wesentlicher Vorteil der Messung der RTT ist, dass keine Zeitsynchronisation der beteiligten Stationen vorausgesetzt wird. Die Messung der RTT geschieht daher lokal auf einer Station. Das bedeutet, dass die Station ein Paket aussendet und gleichzeitig die Zeit speichert, zu der das Paket ausgesendet wurde. Sobald sie auf das ausgesendete Paket eine Antwort erhält, kann sie die Differenz zwischen diesen beiden Zeiten berechnen. Das Resultat dieser Berechnung ergibt dann die RTT. Die RTT wird in diesem Mess-Setup mittels zweier Verfahren gemessen. Das erste Verfahren basiert auf der Verwendung von ICMP-Paketen und das zweite auf dem TCP-Protokoll.

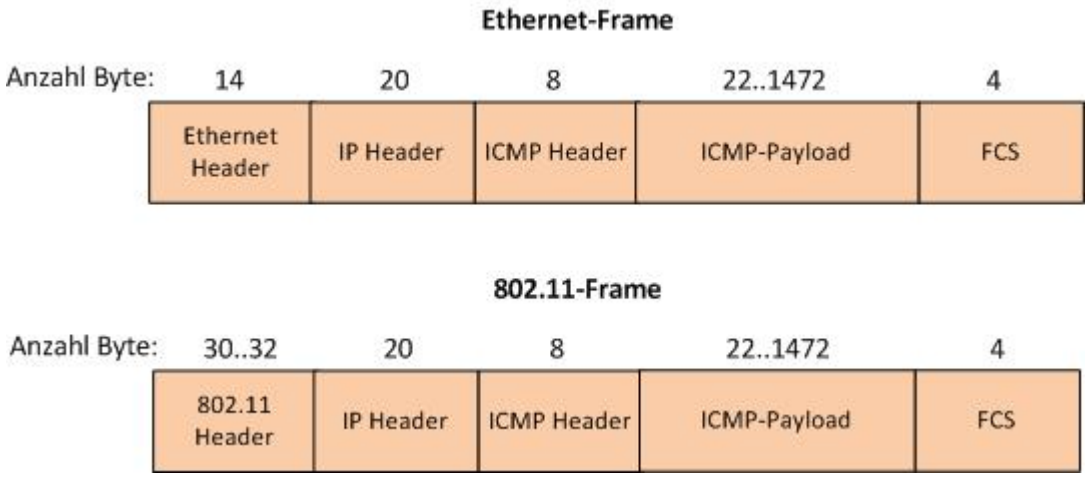
Bei der Berechnung der RTT mittels ICMP-Paketen werden nacheinander ICMP-Pakete vom Notebook 1 an das Notebook 2 gesendet. Um diese Messung automatisiert durchzuführen, wurde folgendes Linux-Skript implementiert:

```
#!/bin/bash
for i in {22..1472..50} do
    ping –c 10 –s $i $1
done
```

Dieses Skript sendet in regelmässigen Zeitabständen ICMP-Pakete an das Notebook 2. Die For-Schleife dient dazu, den ICMP-Payload bei jedem Durchgang der Schleife zu erhöhen, bis die maximale ICMP-Payload-Länge von 1472 Byte erreicht wurde. Im obigen Skript beginnt der ICMP-Payload bei 22 Byte und wird bei jedem Durchlauf um 50 Byte erhöht. Die aktuelle Länge des Payloads wird in der Variablen i zwischengespeichert. Innerhalb der For-Schleife wird der Ping ausgeführt. Dazu werden die Optionen –c und –s benutzt. Das –c 10 legt fest, dass zehn ICMP-Pakete an das Ziel gesendet werden sollen. Die Option –s $i gibt den ICMP-Payload für jeden Durchlauf der Schleife an. Dabei bedeutet das Dollarzeichen, dass der Wert der Variablen i verwendet werden soll. Mittels des $1 kann beim Ausführen des Programms ein Kommandozeilenargument mitgegeben werden. So kann beim Ausführen des Skriptes die IP-Adresse des Empfängers angegeben werden. Beispielsweise ./skriptname 192.168.1.11. Durch dieses Skript ist ersichtlich, ob längere Frames einen Einfluss auf die RTT haben und wenn ja, wie viel.

Die maximale Länge des ICMP-Payloads von 1472 Byte ergibt sich daraus, dass die für diese Arbeit verwendeten Netzwerkkarten der Notebooks und des Access Point eine maximale MTU von 1500 Byte unterstützen. Die MTU ist die maximale Paketgrösse auf dem Network-Layer, welche ohne Fragmentierung in ein Frame auf dem Data-Link-Layer passt. Bei einem Ping wird der ICMP-Payload noch mit einem ICMP-Header (acht Byte) und einem IP-Header (20 Byte) auf dem Network-Layer ergänzt. Durch die Summierung des maximalen ICMP-Payloads von 1472 Byte und der Header von ICMP und IP ergibt sich somit eine MTU von 1500 Byte. Würde diese Grösse überschritten, müssten sowohl der Access Point als auch das Notebook eine Fragmentierung bzw. Defragmentierung durchführen. Die Fragmentierung und die Defragmentierung beanspruchen wiederum Zeit, was sich negativ auf die Geschwindigkeit des Netzwerks auswirken würde, da dieser Prozess auf dem Access Point

und auf dem Notebook Bearbeitungszeit beansprucht. Der genaue Aufbau eines Frames unter Verwendung des ICMP-Protokolls ist in der untenstehenden Abbildung dargestellt.



Bei der Bildung eines Ethernet-Frames wird das Paket noch mit einem Ethernet-Header und einer FCS ergänzt. Somit ergibt sich eine maximale Ethernet-Frame-Länge von 1518 Byte. Hingegen kann das 802.11-Frame bei einer MTU von 1500 Byte bis zu 1536 Byte lang werden, da der 802.11-Header mit einer Länge von 30 bzw. 32 Byte grösser ist als derjenige bei Ethernet. Auch hier wird noch eine FCS von vier Byte angehängt.

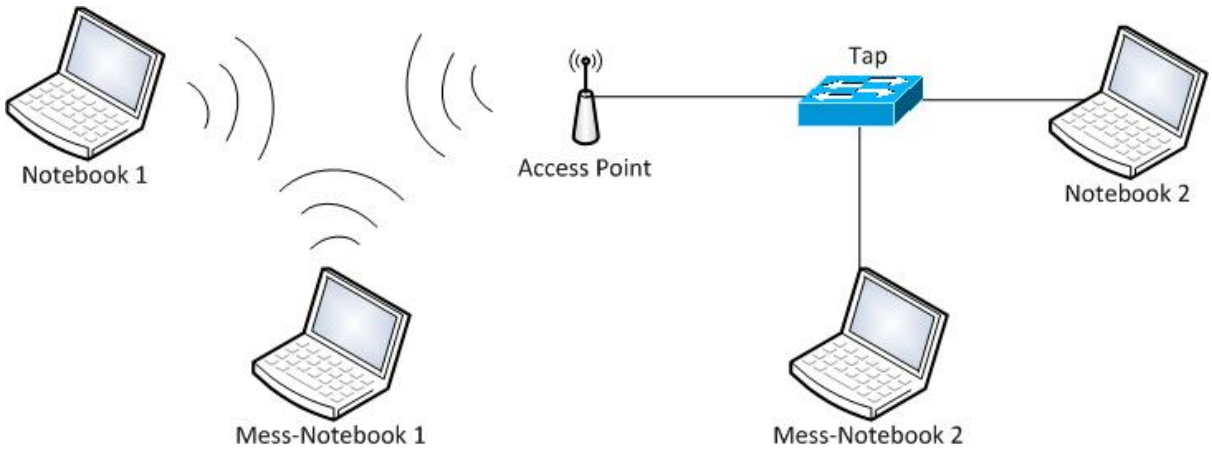
Um die RTT auf dem Transport-Layer zu erhalten, wird das TCP Three-Way-Handshake verwendet. Dabei sendet die Station, die eine Verbindung aufzubauen versucht, ein TCP SYN. Dadurch registriert die Empfängerstation, dass versucht wird, mit ihr eine Verbindung aufzubauen. Die empfangende Station bestätigt dies mit einem TCP SYN-ACK. Durch den Erhalt des TCP SYN-ACK erfährt der Initiant der Verbindung, dass die Verbindungsanfrage vom Empfänger bestätigt wurde und dieser bereit ist, Daten zu empfangen. Um den Three-Way-Handshake abzuschliessen, bestätigt die initiierende Station den Erhalt des TCP SYN-ACK mittels eines TCP ACK. Nachdem das TCP ACK empfangen worden ist, sind die Stationen bereit, Daten bidirektional auszutauschen. Durch den Three-Way-Handshake ist es somit möglich, die RTT auf dem Transport-Layer zu bestimmen. Dazu wird auf Notebook 1 und Notebook 2 das Programm Wireshark benutzt, um einen TCP-Verbindungsaufbau aufzuzeichnen. Wireshark bietet die Möglichkeit, den Three-Way-Handshake aufzuzeichnen, und berechnet zusätzlich dessen RTT. Um eine TCP-Verbindung zwischen den Notebooks aufzubauen, wird hier das Programm IPerf verwendet. Dazu wird das Notebook 1 als Client und das Notebook 2 als Server konfiguriert und eine Datenübertragung durchgeführt. Damit eine statistische Aussage über die RTT gemacht werden kann, wird auch hier zehn Mal eine TCP-Verbindung aufgebaut und mit Wireshark aufgezeichnet und die RTT analysiert und dokumentiert.

MESSUNG DER VERARBEITUNGSZEIT

Die Verarbeitungszeit von netzwerkfähigen Geräten hat einen grossen Einfluss darauf, welche Geschwindigkeit in einem Netzwerk maximal erreicht werden kann. Diese Verarbeitungszeit hängt jeweils vom verwendeten Protokoll-Stack ab. Der Protokoll-Stack ist je nach Implementierung unterschiedlich. Somit haben die meisten Betriebssysteme unterschiedliche Protokoll-Stacks. Dies erschwert eine genaue Aussage über die Verarbeitungszeit. Die Verarbeitungszeit ist die Zeitdauer, welche ein Gerät benötigt, um die Daten zu empfangen und zu verarbeiten und gegebenenfalls eine Antwort zu senden. Dabei wird der Protokoll-Stack zweimal durchlaufen, erstens beim Empfang der Daten und zweitens beim Aussenden der Daten. Jeder Layer fügt den Daten Kontrollinformationen hinzu. Beispielsweise fügt der Layer 3 den IP-Header und der Layer 2 einen MAC-Header und Trailer hinzu. Somit ist die Summe aller Zeitabschnitte, welche ein Layer zur Abarbeitung seiner Aufgabe benötigt, die Gesamtverarbeitungszeit des jeweiligen Protokoll-Stacks.

Um die Verarbeitungszeit der verwendeten Geräte annähernd zu bestimmen, werden im Mess-Setup an verschiedenen Stellen Frames aufgezeichnet. Dadurch ist ersichtlich, zu welchem Zeitpunkt ein Frame bei einer Komponente empfangen wurde und zu welchem Zeitpunkt es von der Komponente weitergeleitet wurde. Somit erhält man annäherungsweise die Verarbeitungszeit der jeweiligen Komponente.

Für die Messung der Verarbeitungszeiten der verschiedenen Komponenten wird folgendes Setup verwendet:



Das Notebook 1 sendet in regelmässigen Zeitabständen ICMP-Pakete an das Notebook 2. Die ICMP-Pakete werden auf beiden Notebooks mit dem Programm Wireshark aufgezeichnet. Durch die Aufzeichnung der ICMP-Pakete erfährt man gleichzeitig auch die Zeit, die ein Paket benötigt, um von der Quelle zum Ziel und zurück zu reisen (Round Trip Time). Damit man nun die Verarbeitungszeit einer Komponente berechnen kann, werden an zwei weiteren Stellen die übertragenen ICMP-Pakete aufgezeichnet. Das Mess-Notebook 1 zeichnet die Pakete während der Übertragung an der Luftschnittstelle auf. Das Mess-Notebook 2 zeichnet die ICMP-Pakete auf dem Kabel auf. Das Mess-Notebook 2 ist an den Tap angeschlossen. Bei einem Tap handelt es sich um ein Gerät, das alle erhaltenen Datenpakete an einen Port weiterleitet, mit dem der Verkehr aufgezeichnet werden kann. Diese zwei zusätzlichen Aufzeichnungen führen dazu, dass man annäherungsweise die Verarbeitungszeit der

einzelnen Komponenten erhält. Somit kann man die Verarbeitungszeiten in Erfahrung bringen, die ein Notebook benötigt, um ein ICMP-Paket zu erhalten und darauf eine Antwort zu senden. Des Weiteren kann die Zeitdauer abgeschätzt werden, die der Access Point benötigt, um ein Frame zu empfangen, zu bearbeiten und weiterzuleiten.

SYNCHRONISATION DER UHREN

Für die Messung der Verzögerung ist es wichtig, dass alle mitwirkenden Stationen im Besitz derselben Uhrzeit sind. Um die Uhren zu synchronisieren, gibt es zwei Möglichkeiten, die hier beschrieben werden.

NETWORK TIME PROTOCOL (NTP)

NTP ist ein Protokoll, das zur Synchronisierung der Zeit in einem Computernetzwerk verwendet werden kann. Um die Uhren zu synchronisieren, gibt es einen lokalen Server. Dieser Server ist dafür verantwortlich, den Stationen die Zeit zukommen zu lassen. Um den Stationen die Zeit zu übermitteln, wird das UDP-Protokoll verwendet. Der Inhalt eines NTP-Pakets enthält dabei einen Zeitstempel, der 64 Bit lang ist. Von diesen 64 Bit werden 32 Bit für die Kodierung der Sekunden seit dem 1. Januar 1900 benötigt. Die restlichen 32 Bit werden für den Sekundenbruchteil verwendet. Der Sekundenbruchteil ist dabei die Auflösung und beträgt 0.32 Nanosekunden. Mittels NTP lässt sich somit ein Zeitraum von 136 Jahren darstellen. Die Genauigkeit der Uhren liegt in lokalen Netzwerken ungefähr bei zehn Millisekunden. Ein Vorteil von NTP ist, dass damit für die Synchronisation der Uhrzeit innerhalb eines Computernetzwerks keine zusätzliche Hardware angeschafft werden muss und auf allen Netzwerkgeräten und Stationen ein NTP-Server angegeben werden kann.

GLOBAL POSITIONING SYSTEM (GPS)

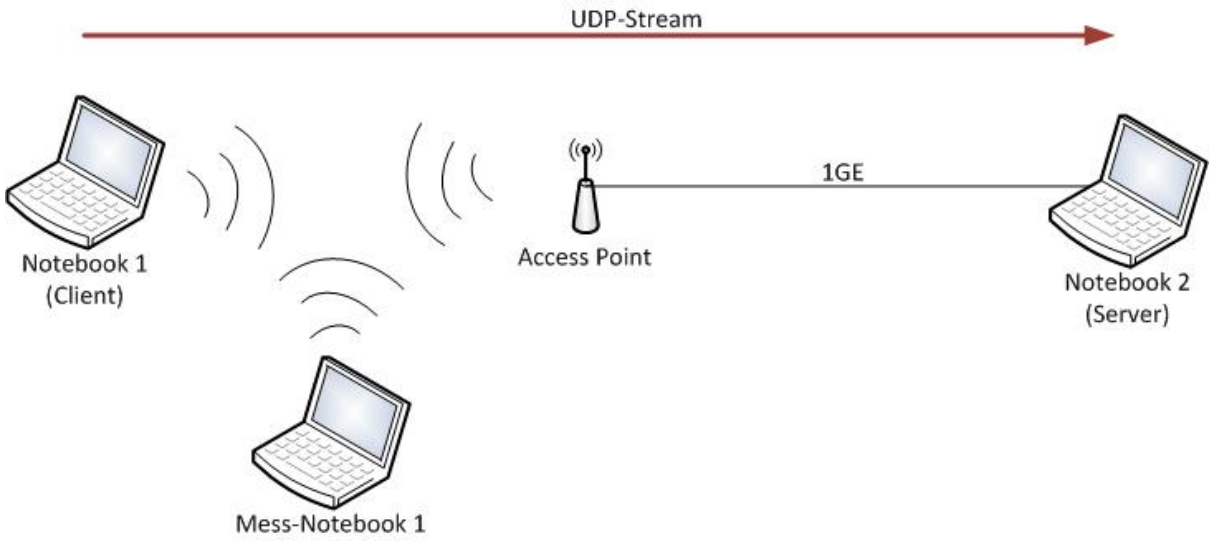
Eine weitere Möglichkeit, um die Zeit innerhalb eines Computernetzwerks zu synchronisieren, ist die Verwendung von GPS. Einfach ausgedrückt wird bei GPS die Laufzeit des Signals vom Satelliten zum GPS-Empfänger berechnet. Die Satelliten senden dabei ihre Zeit an die Stationen aus. Die GPS-Empfänger berechnen nach Erhalt der Satellitenzeit ihre lokale Zeit. Hierfür wird die Satellitenzeit mit der Laufzeit addiert und die Empfänger erhalten dadurch die exakte Uhrzeit. Mittels GPS kann eine Zeitgenauigkeit von einer µs erreicht werden. Eine Voraussetzung für die Zeitsynchronisation mittels GPS ist aber, dass jede Station und jede Netzwerkkomponente mit einem GPS-Empfänger ausgestattet ist. Da die in dieser Arbeit verwendeten Access Points keine Möglichkeit bieten, einen GPS-Empfänger anzuschliessen, kann die Zeit hier nicht mittels GPS berechnet werden.

Es gibt zahlreiche Anbieter von GPS-Empfängern. Hier ein Link zu einem Produkt der Firma Hama:

http://www.hama.de/00053118/hama-gps-empfaenger-usb

MESSSZENARIEN

Für die nachfolgenden Szenarien wird das im Kapitel „Messaufbau“ beschriebene Setup verwendet. Bei allen Szenarien ist das Notebook 1 der IPerf-Client und das Notebook 2 der IPerf Server. Das Notebook 1 sendet bei den verschiedenen Messungen einen UDP-Stream an das Notebook 2 mit einer Zeitdauer von 30 Sekunden. Jedes UDP-Paket hat eine Länge von 1472 Byte, sodass die MTU von 1500 Byte ausgenutzt wird. Das Mess-Notebook 1 dient dazu, den Verkehr zwischen dem Notebook 1 und dem Access Point mittels AirPCAP-Adapter und Wireshark aufzuzeichnen.



G-STANDARD

Im G-Standard wurden hauptsächlich Anpassungen auf dem Physical-Layer getätigt. Um die Auswirkungen dieser Anpassungen analysieren zu können, werden verschiedene Messungen durchgeführt. In den unten aufgeführten Szenarien wird auf dem Access Point nur das 802.11bg aktiviert. Des Weiteren wird auf dem Access Point der E-Standard deaktiviert, um sicherzustellen, dass nur der G-Standard aktiv ist.

PREAMBLE

Um die Auswirkung der zwei verschiedenen Längen der Präambel auf die WLAN-Performance analysieren zu können, werden zwei Messungen durchgeführt und miteinander verglichen. Bei der ersten Messung wird eine lange Präambel (72 µs) verwendet. Bei der zweiten Messung wird eine kurze Präambel (20 µs) eingestellt.

RTS-/CTS-MECHANISMUS

Diese Messung untersucht den Einfluss der Verwendung des RTS/CTS-Mechanismus auf den Durchsatz innerhalb eines WLANs. Dazu wird ein Vergleich zwischen aktiviertem und deaktiviertem RTS/CTS Mechanismus durchgeführt. Der RTS-Threshold wird auf 1500 Byte gestellt. Dies führt dazu, dass ab einer Framelänge von 1500 Byte der RTS/CTS-Mechanismus aktiviert wird.

E-STANDARD

Der E-Standard erweitert den G-Standard um weitere Optimierungen auf dem Data-Link-Layer. Zu den Optimierungen gehören unter anderem die Unterstützung der Dienstgüte (QoS) durch einen effizienteren Medienzugriff, das Senden von Bursts sowie die Bestätigung von mehreren empfangenen Frames durch ein einzelnes ACK-Frame. Um die Effizienzsteigerung des E-Standards zu bestimmen, werden die Messungen des G-Standards mit aktiviertem E-Standard wiederholt. Dabei wird der E-Standard auf dem Access Point aktiviert. Es gibt auf dem Access Point keine Möglichkeit, das Block-Acknowledgement zu deaktivieren. Dies führt dazu, dass es bei der Aktivierung des E-Standards automatisch aktiv ist.

BLOCK-ACKNOWLEDGEMENT

Um die Auswirkung des Block-Acknowledgement auf den WLAN-Durchsatz zu ermitteln, werden die Szenarien des G-Standards mit aktiviertem E-Standard wiederholt durchgeführt. Zusätzlich wird das Bursting auf dem Access Point deaktiviert. Durch die Deaktivierung des Bursting ist sichergestellt, dass nur das Block-Acknowledgement bei der Messung aktiv ist.

BURSTING

Eine weitere Messung des E-Standards erfolgt unter Benutzung des Bursting, um dessen Effekt zu ermessen. Dazu wird auf dem Access Point das TXOP-Limit auf das Maximum gestellt und die Messungen des G-Standards werden ein weiteres Mal durchgeführt.

EDCA-PARAMETER

Mithilfe dieses Szenarios wird überprüft, wie der Medienzugriff durch die Priorisierung von Daten beschleunigt wird. Um dies realisieren zu können, wird ein Voice- und Video-Stream unter Benutzung von IPerf simuliert. Da mittels IPerf keine Priorisierung von IP-Paketen eingestellt werden kann, ist es für den Access Point nicht möglich, diese Pakete zu priorisieren. Aus diesem Grund werden für diese Tests die AIFS, CWmin, CWmax und das TXOP-Limit entsprechend den vordefinierten Verkehrsklassen für Voice und Video auf dem Access Point konfiguriert. Das heisst, dass diese vordefinierten Werte in die Data0 Queue „Best Effort“ eingefügt werden. Dies führt dazu, dass die IP-Pakete innerhalb der Queue „Data0“ durch die entsprechenden Werte priorisiert werden.

N-STANDARD

Der N-Standard verspricht einige Verbesserungen auf dem Physical-Layer sowie auch auf dem Data-Link-Layer, um den Datendurchsatz innerhalb eines WLAN-Netzwerks zu beschleunigen. In den nachfolgend beschriebenen Szenarien geht es in erster Linie darum, herauszufinden, welche Verbesserung welchen Einfluss auf den Durchsatz in WLAN-Netzwerken hat. Da der N-Standard sowohl den 2.4-GHz- als auch den 5-GHz-Bereich benutzt, werden die nachfolgenden Messszenarien in beiden Frequenzbereichen durchgeführt. Zusätzlich werden die Messungen jeweils einmal ohne und einmal mit Kanalbündelung durchgeführt.

GUARD INTERVAL

Das Guard Interval ist die Zeitdauer, die zwischen zwei OFDM-Symbolen mit dem Absenden abgewartet werden muss. Diese Zeitdauer hat einen wesentlichen Einfluss auf die zu erreichende Geschwindigkeit in einem WLAN. Beim Access Point kann dieses Guard Interval konfiguriert werden. Dabei kann zwischen zwei Intervallen ausgewählt werden. Das erste Intervall ist das Long Guard Interval und hat eine Zeitdauer von 800ns. Das zweite ist das Short Guard Interval mit einer Zeitdauer von 400ns. Um die Steigerung des Durchsatzes bei Verwendung des entsprechenden Guard Interval zu erhalten, werden zwei Messungen durchgeführt, eine unter Verwendung des Short Guard Interval und eine mit Long Guard Interval.

FRAME-AGGREGATION

Die Aggregation von Frames verspricht eine Steigerung des Durchsatzes aufgrund der Tatsache, dass bis zu 64 Frames zu einem einzigen Frame aggregiert werden können. Dieses aggregierte Frame hat den Vorteil, dass nur ein Header (Layer 1 und Layer 2) hinzugefügt wird. Des Weiteren muss eine Station nur einmal den Zugriff auf das Medium erhalten, damit das aggregierte Frame übertragen werden kann. Dies führt zu einer wesentlichen Effizienzsteigerung in Bezug auf die Datenübertragungsrate. Um diese Steigerung der Effizienz zu messen, wird in dieser Messung einmal ein Stream von Daten mit und einmal einer ohne Aggregation von Frames durchgeführt. Dazu wird auf dem Access Point die A-MPDU aktiviert und deaktiviert. Diese Messungen werden nur unter Verwendung des Short Guard Interval durchgeführt.

RIFS

Mittels RIFS wird die Zeit zwischen der Aussendung zweier nicht aggregierter Frames verkürzt. Ist RIFS deaktiviert, so muss nach dem Aussenden eines Frames jeweils eine SIFS-Zeitdauer abgewartet werden, bevor das nächste Frame gesendet werden kann. Im 2.4-GHz-Bereich beträgt diese Zeitdauer zehn µs, im 5-GHz-Bereich sogar 16 µs. Bei aktiviertem RIFS muss nur noch für zwei µs gewartet werden. Somit ist die Wartezeit zwischen zwei aufeinanderfolgenden Frames um den Faktor 5 bzw. 8 verkürzt und es kann eine grössere Anzahl Frames pro Sekunde ausgesendet werden. Um die Erhöhung des Durchsatzes mittels RIFS zu ermitteln, wird hier eine Vergleichsmessung zwischen aktiviertem und deaktiviertem RIFS durchgeführt. Für die Messung des RIFS ist es notwendig, die Aggregati-

on von Frames auf dem Access-Point zu deaktivieren. Auch bei diesem Szenario werden die Messungen nur mit dem Short Guard Interval durchgeführt.

MESSUMGEBUNG

Die oben beschriebenen Messszenarien werden in zwei verschiedenen Umgebungen durchgeführt. Zum Einen in einem Unterrichtszimmer und zum Anderen in einer HF-Kammer.

UNTERRICHTSZIMMER

Die Ausführung der Messungen im Unterrichtszimmer erlaubt die Analyse von WLANs, wie sie unter normalen Bedingungen in der Realität anzutreffen sind. Das hat zur Folge, dass mit Interferenzen und anderen Störeinflüssen gerechnet werden muss. Diese Störeinflüsse können das Messergebnis verfälschen. Zu den Störeinflüssen gehören unter anderem Personen, vorhandene WLANs und der Raum. Deshalb ist es schwierig bzw. fast unmöglich, genaue Aussagen über die Datenübertragung von WLANs zu machen, da viele verschiedene Faktoren von grosser Bedeutung sind.

Das untenstehende Bild veranschaulicht die Ausgangslage, bevor mit den Messungen begonnen wurde. Hier sind alle im Raum vorhandenen WLANs aufgelistet. Des Weiteren werden zu jedem WLAN auch die Signalstärke und das Signal-Rausch-Verhältnis angezeigt.

SSID	Signal	Signal Avg	Signal Max	Noise	Channel	BSSID	Enc Type	Spec	Last Seen
HSR-Secure	6%	6%	6%	6%	44	6C:50:4D:AB:9B:3C	WPS	802.11n	21.05.12 16:48:38
HSR-WLAN	11%	10%	11%	9%	36	6C:50:4D:AB:13:CE	None	802.11n	21.05.12 16:48:38
MOBILE-EAPSIM	9%	10%	10%	9%	36	6C:50:4D:AB:13:CB	WEP	802.11a	21.05.12 16:48:38
HSR-WLAN	18%	17%	18%	12%	11	6C:50:4D:AB:9C:61	None	802.11n	21.05.12 16:48:38
HSR-WLAN	36%	36%	36%	12%	11	6C:50:4D:AB:8C:A1	None	802.11n	21.05.12 16:48:38
MOBILE-EAPSIM	36%	36%	36%	12%	11	6C:50:4D:AB:8C:A4	WEP	802.11g	21.05.12 16:48:38
eduroam	36%	36%	36%	4%	11	6C:50:4D:AB:8C:A5	WPS	802.11n	21.05.12 16:48:38
eduroam	16%	16%	16%	10%	11	6C:50:4D:AB:9C:65	WPS	802.11n	21.05.12 16:48:38
HSR-Secure	18%	18%	18%	12%	11	6C:50:4D:AB:9C:63	WPS	802.11n	21.05.12 16:48:38
HSR-WLAN	18%	18%	18%	16%	6	6C:50:4D:AB:9B:31	None	802.11n	21.05.12 16:48:38
HSR-Secure	18%	18%	18%	13%	6	6C:50:4D:AB:9B:33	WPS	802.11n	21.05.12 16:48:38
eduroam	18%	18%	18%	13%	6	6C:50:4D:AB:9B:35	WPS	802.11n	21.05.12 16:48:38
MOBILE-EAPSIM	18%	18%	18%	13%	6	6C:50:4D:AB:9B:34	WEP	802.11g	21.05.12 16:48:38
HSR-WLAN	22%	22%	23%	12%	1	6C:50:4D:AB:9B:41	None	802.11n	21.05.12 16:48:38
eduroam	60%	60%	60%	10%	1	6C:50:4D:AB:7F:C4	WPS	802.11n	21.05.12 16:48:38
HSR-WLAN	48%	42%	48%	12%	1	B4:14:89:14:37:61	None	802.11n	21.05.12 16:48:38
HSR-Secure	34%	34%	34%	10%	1	B4:14:89:14:37:13	WPS	802.11n	21.05.12 16:48:38
HSR-WLAN	36%	34%	36%	12%	1	B4:14:89:14:37:11	None	802.11n	21.05.12 16:48:38
HSR-WLAN	59%	60%	60%	12%	1	6C:50:4D:AB:7F:C1	None	802.11n	21.05.12 16:48:38
HSR-WLAN	20%	19%	20%	12%	1	6C:50:4D:AB:13:C1	None	802.11n	21.05.12 16:48:38
eduroam	18%	18%	18%	12%	1	6C:50:4D:AB:13:C5	WPS	802.11n	21.05.12 16:48:38
HSR-Secure	61%	61%	61%	4%	1	6C:50:4D:AB:7F:C8	WPS	802.11n	21.05.12 16:48:38
eduroam	34%	34%	34%	4%	1	B4:14:89:14:37:15	WPS	802.11n	21.05.12 16:48:38
HSR-Secure	17%	17%	17%	12%	1	6C:50:4D:AB:13:C3	WPS	802.11n	21.05.12 16:48:38
MOBILE-EAPSIM	36%	36%	36%	12%	1	B4:14:89:14:37:64	WEP	802.11g	21.05.12 16:48:38
MOBILE-EAPSIM	60%	60%	60%	12%	1	6C:50:4D:AB:7F:C2	WEP	802.11g	21.05.12 16:48:38
MOBILE-EAPSIM	16%	16%	16%	12%	1	6C:50:4D:AB:13:C4	WEP	802.11g	21.05.12 16:48:38
HSR-WLAN	19%	19%	19%	10%	1	6C:50:4D:B7:99:E1	None	802.11n	21.05.12 16:48:38
eduroam	52%	52%	52%	12%	1	B4:14:89:14:37:65	WPS	802.11n	21.05.12 16:48:38

HF-KAMMER

Die zweite Umgebung, in der die Messungen durchgeführt wurden, ist eine HF-Kammer der HSR (Hochschule für Technik Rapperswil). Diese Kammer bietet eine elektromagnetische Schirmung, mit der Störeinflüsse von aussen vermieden werden. Das bedeutet, dass innerhalb der Kammer keine Strahlung von aussen vorhanden ist. Ohne Störeinflüsse aus der Umgebung kann eine genauere Analyse von WLANs vorgenommen werden und die Messresultate werden reproduzierbar. Die folgenden Bilder zeigen das Innenleben dieser HF-Kammer. Die gräulichen bzw. bläulichen Pyramiden sind sogenannte Breitbandabsorber. Die Funktion dieser Absorber ist die Absorption der ausgestrahlten Signale, sodass diese an den Wänden nicht reflektiert werden. Die Absorber bestehen aus Schaumstoff, welcher mit einer speziellen leitfähigen Legierung bestrichen ist.

MESSAUSWERTUNG

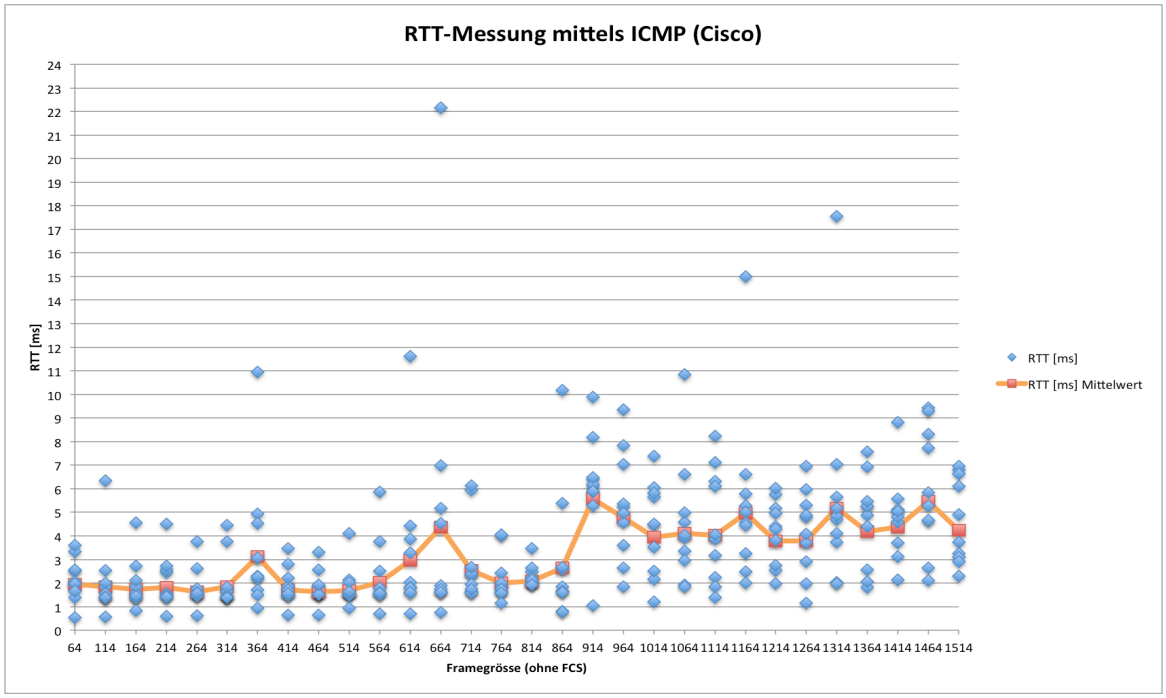
ROUND TRIP TIME MIT ICMP

In den unten abgebildeten Diagrammen sind jeweils die Round-Trip-Zeiten unter Verwendung des ICMP-Protokolls dargestellt.

Bei allen dieser Messungen ist zu erkennen, dass mit zunehmender Frame-Länge auch die Verarbeitungszeit zunimmt. Der Grund dafür ist, dass die Verarbeitung von langen Frames mehr Zeit in Anspruch nimmt als jene von kurzen Frames. Eine Station benötigt bei langen Frames mehr Zeit, um das gesamte Frame zu senden oder zu empfangen, da eine grössere Anzahl von Bytes übertragen wird. Ein weiterer Faktor ist die Verarbeitungszeit beim Access Point. Der Access Point empfängt das Frame, welches über die Luft gesendet wurde, und führt danach eine Medienkonvertierung durch. Beim Hinweg findet eine Konvertierung von 802.11 nach Ethernet statt, beim Rückweg eine solche von Ethernet zu 802.11. Diese Konvertierung benötigt auch wieder Zeit. Zusätzlich muss der Access Point nach der Konvertierung das Frame wieder auf das Medium legen und dem Empfänger zusenden. Die Zeitdauer, welche benötigt wird, um ein Frame auf das Medium zu legen, wird Serialisierungszeit genannt. Um diese zu bestimmen, muss die Frame-Länge mit der Bitzeit multipliziert werden. Die Bitzeit ist die Umkehrfunktion der Bitrate. Für einen Gigabit-Link wäre die Bitzeit somit: *1/1000000000 = 1 ns.* Daraus würde sich für ein Frame der Länge von 1514 Byte eine Bitzeit von 12,112 µs ergeben.
Ein weiterer Grund für die Ausreisser ist, dass der ARP-Cache der Notebooks auf 30 Sekunden eingestellt ist. Somit senden diese Stationen alle 30 Sekunden einen ARP-Request aus und erhalten als Antwort eine ARP-Response. Eine Messung für eine Frame-Länge dauert 10 Sekunden. Somit wird während jeder dritten Messung ein ARP-Request gesendet.

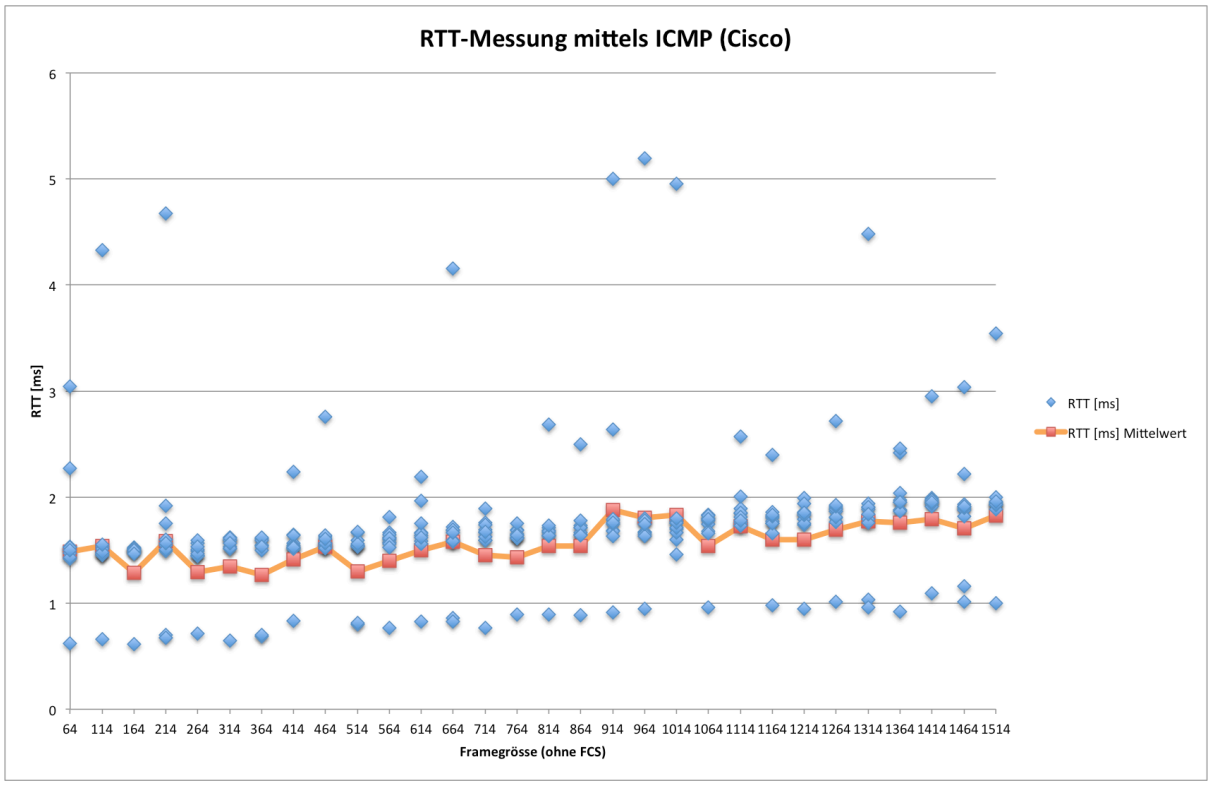
CISCO

GESTÖRTES UMFELD



Im gestörten Umfeld ist ersichtlich, dass zwischendurch kleinere und grössere Ausreisser vorkommen. Diese sind auf Störeinflüsse wie Interferenzen bzw. andere aktive WLAN-Stationen zurückzuführen.

HF-KAMMER

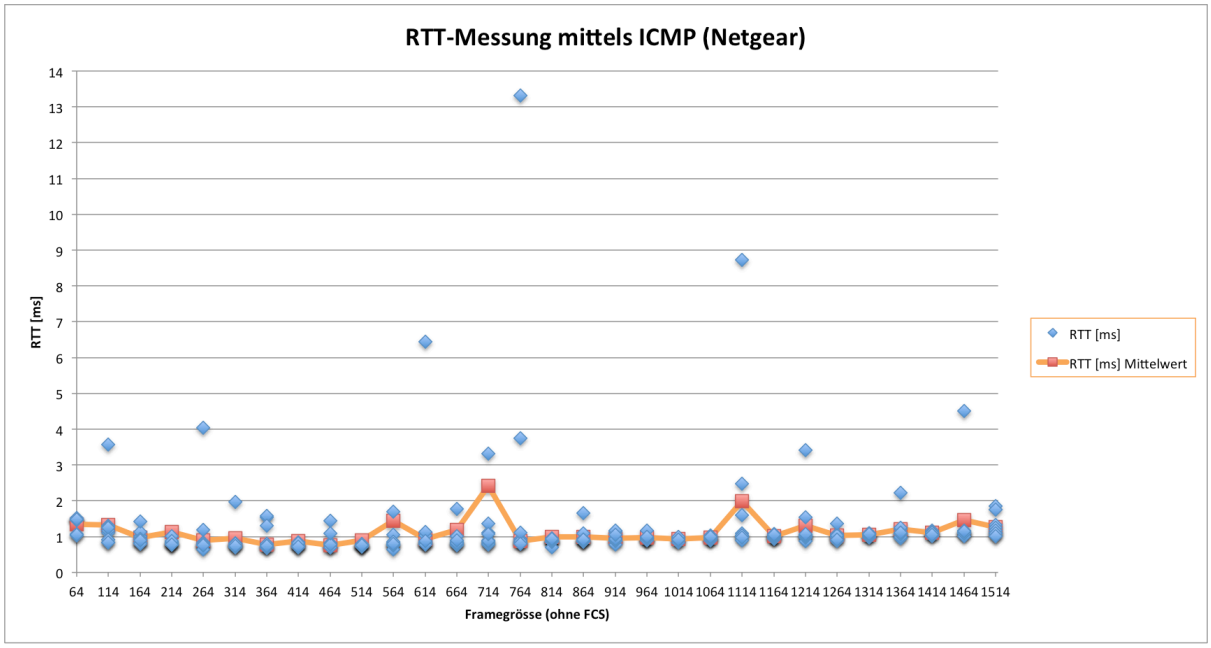


Die Auswertung der RTT innerhalb der HF-Kammer zeigt grosse Unterschiede zum gestörten Umfeld. Hier ist ersichtlich, was für einen Einfluss Interferenzen auf WLANs haben. Die RTT-Werte liegen hier zwischen 0.7 und 5.1 ms. Im gestörten Umfeld waren sie zwischen 0.7 und 22 ms. Auch in der HF-Kammer sind wieder Ausreisser vorhanden, diese sind auf Schwankungen der Verarbeitungszeit zurückzuführen. Neben der Serialisierungszeit und der Konvertierungszeit sind auch die zu verwendenden Backoff-Zeiten der Stationen und des Access Point Ursachen für diese Schwankungen. Wie im Kapitel Grundlagen erläutert, erteilt der Backoff-Algorithmus den Stationen einen TimeSlot, in dem sie auf das Medium zugreifen dürfen. Nun kann es vorkommen, dass eine Station unmittelbar einen TimeSlot zugewiesen bekommt und deshalb auf das Medium zugreifen darf. Allerdings ist es auch möglich, dass eine Station bzw. ein Access Point den letzten TimeSlot erhält und deshalb warten muss, bis sie auf das Medium zugreifen darf. Dies führt dann zu Zeitschwankungen beim Aussenden von Frames, was sich auch in den RTT-Werten widerspiegelt.

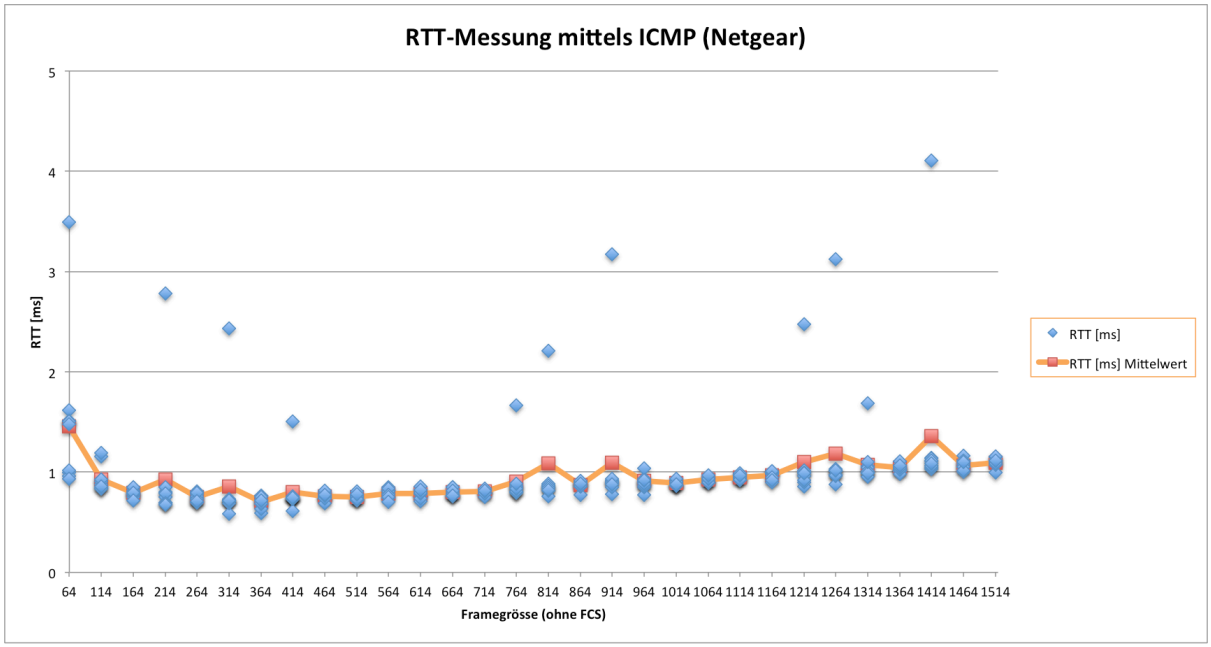
NETGEAR

Bei der Messung der Round Trip Time unter Verwendung des Netgear Access Point ist ersichtlich, dass die RT-Zeiten kürzer sind als beim Cisco Access Point. Somit lässt sich sagen, dass die Verarbeitungszeit beim Netgear Access Point kürzer ist, als es beim Cisco-AP der Fall ist. Die RTT-Werte sind beim Netgear, mit Ausnahme einzelner Ausreisser, sehr konstant. Diese Ausreisser sind das Resultat sowohl von Störeinflüssen als auch der Verarbeitungszeit.

GESTÖRTES UMFELD



HF-KAMMER



Nach der Analyse des Sniffer-Traces wurde ersichtlich, dass beim Punkt mit der Frame-Länge von 64 Byte und einer RTT von 3.4 ms ein ARP-Request/-Response vorausgegangen war. Dies führte zu einem hohen RTT-Wert.

ROUND TRIP TIME MIT TCP

Bei der Messung der Round Trip Time mit dem TCP-Protokoll ist es wichtig zu wissen, dass die Round Trip Time vom Layer 4 abhängig ist.

Vergleicht man die RTT-Werte im gestörten Umfeld mit denen in der HF-Kammer, so ist erneut zu erkennen, dass in einem ungestörten Umfeld die RTT-Werte deutlich tiefer werden.

Um auf eine Ursache schliessen zu können, wurden die Sniffer-Traces ausgewertet. Dazu wurde die Verarbeitungszeit des Notebooks 1 (Client) und des Notebooks 2 (Server) ausgewertet. Es wurde betrachtet, wie viel Zeit vergeht, wenn eine Station ein Frame erhalten hat und darauf eine Antwort zurücksendet.

CISCO

Unten sind die Verarbeitungszeiten von Client und Server aufgelistet.

- Client
  - Min: 1 µs
  - Max: 59 µs
  - Mittelwert: 12 µs
- Server
  - Min: 1 µs
  - Max: 278 µs
  - Mittelwert: 22 µs

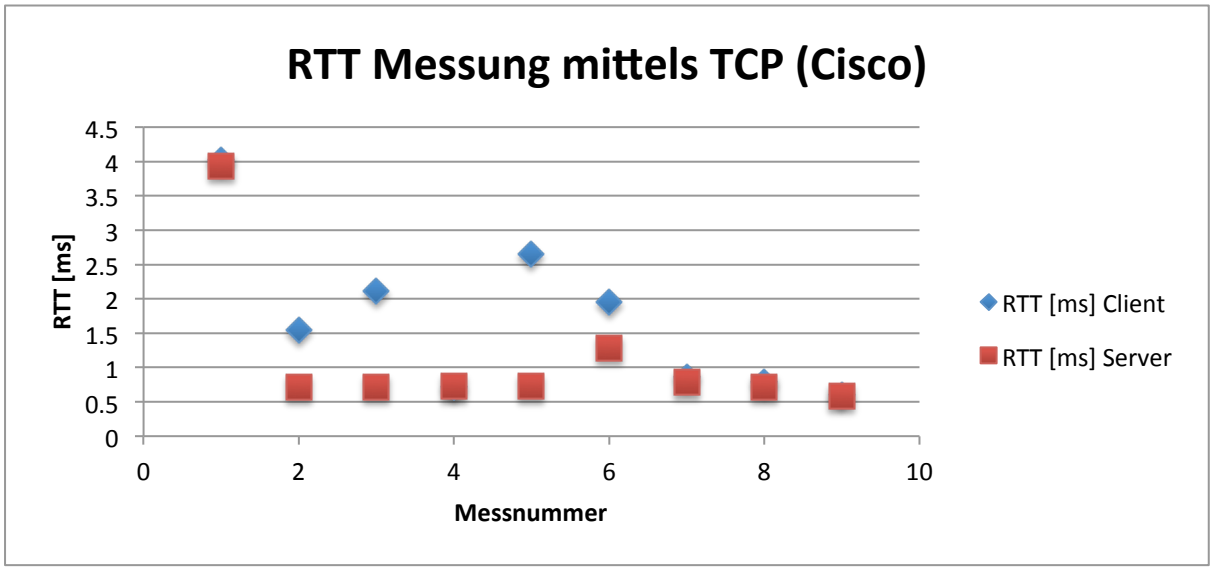
Diese Antwortzeiten deuten darauf hin, dass die Stationen in der Lage sind, in sehr kurzer Zeit Frames zu empfangen und zu verarbeiten und Antworten zurückzusenden. Aus diesem Grund kann ausgeschlossen werden, dass die Stationen einen grossen Einfluss auf die Schwankungen der RTT haben. Dabei bedeutet „grosser Einfluss“ einen Einfluss auf die Schwankungen in Höhe von 2.5 Millisekunden und höher.

In den untenstehenden Diagrammen ist auch ersichtlich, dass beim Server bei der ersten Messung (Messnummer 1) immer ein höherer RTT-Wert vorhanden ist, als es bei den späteren Messnummern der Fall ist. Dies liegt daran, dass der Server bei der ersten Verbindungsanfrage immer einen Puffer im Speicher reservieren muss. Dieser Puffer wird benötigt, um die empfangenen TCP-Segmente kurzfristig darin zu speichern, damit sie in die richtige Reihenfolge gebracht werden können, bevor sie dann der Applikation übergeben werden.

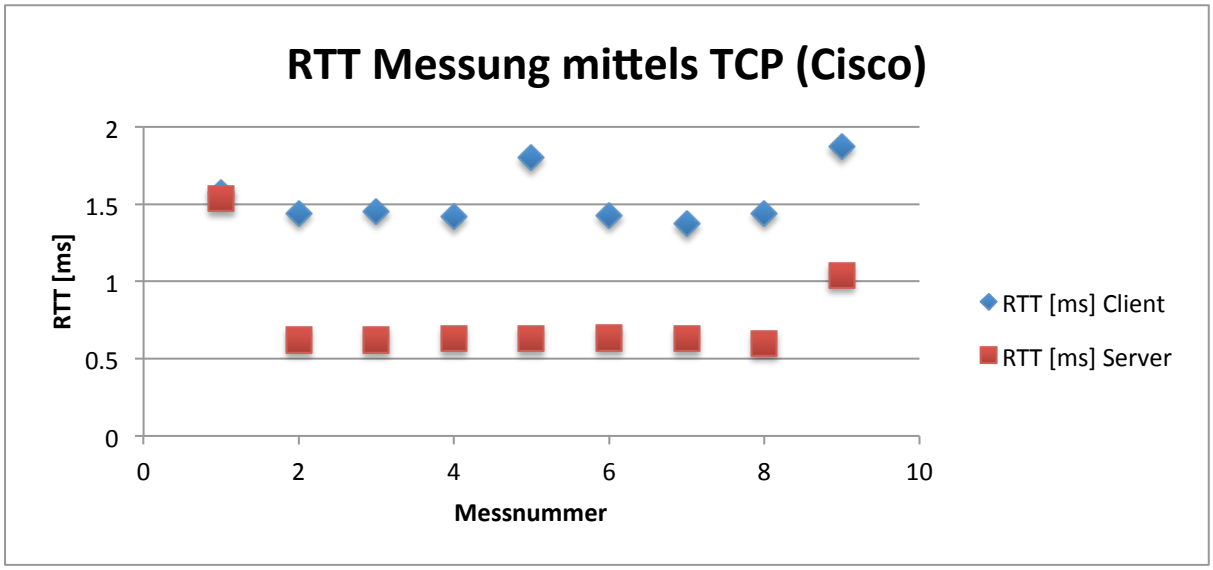
Was beim Cisco Access Point weiter auffällt, ist die Tatsache, dass die RTT-Werte des Servers fast immer tiefer sind als jene des Clients. Das liegt daran, dass der Server dem Access Point via Ethernet die Frames sendet. Diese werden dann in ein 802.11-Frame konvertiert und dem Client gesendet. Beim Zugriff auf das Medium ist der Access Point gegenüber Stationen privilegiert. Das heisst, er hat die höchste Priorität. Diese erhält er deshalb, weil er bei sich die CW-Werte tiefer setzt als bei Stati-

onen und über den Backoff-Algorithmus deshalb immer den Medienzugriff erhält. Diese Tatsache zeigt sich auch, wenn man WLAN-Verkehr snifft. Dabei werden die ACK-Frames innerhalb weniger µs auf das Medium gelegt. Auch dies liegt daran, dass der Access Point eine höhere Priorität hat als die Stationen.

GESTÖRTES UMFELD



HF-KAMMER



In der HF-Kammer sind die RTT-Werte wiederum tiefer als im gestörten Umfeld. Dies bestätigt wiederum, dass die Verarbeitungszeiten der Stationen (Notebook 1 und Notebook 2) keinen grossen Einfluss auf die RTT-Werte haben. Vielmehr sind die Störeinflüsse wie Interferenzen oder die Zugriffszeit auf das Medium für die Verzögerungen verantwortlich.

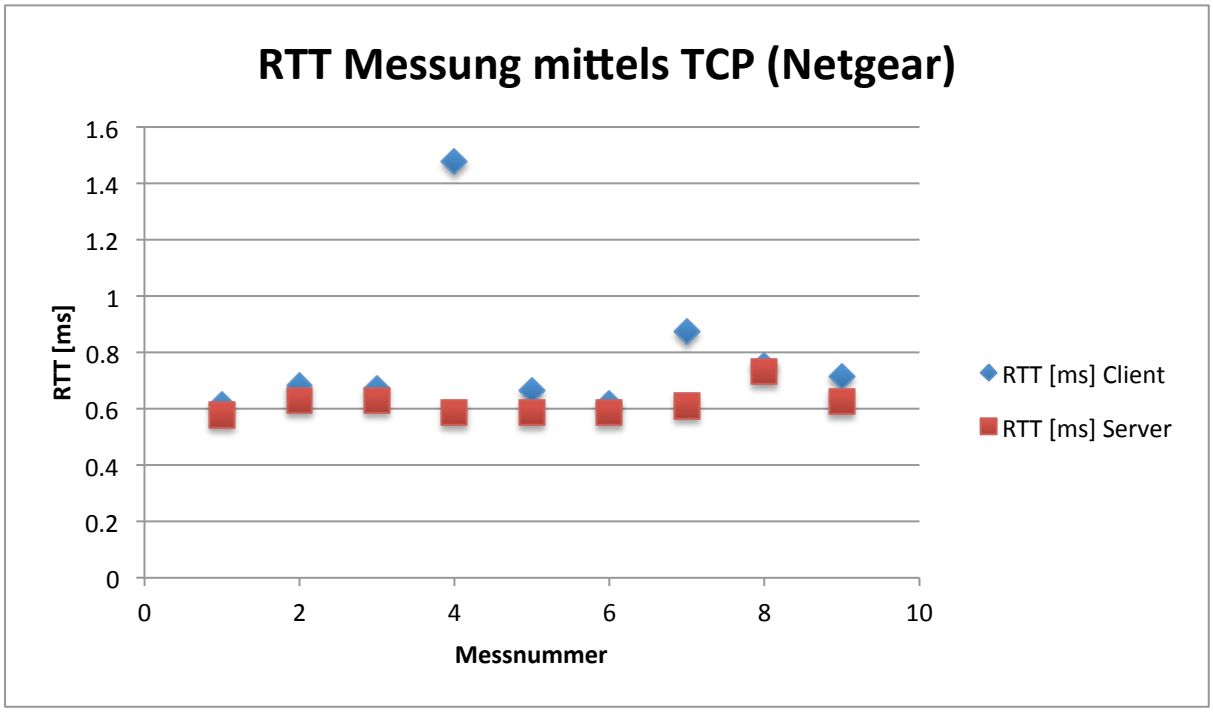
NETGEAR

Nachfolgend sind die Antwortzeiten von Client und Server aufgelistet.

- Client
  - Min: 5 µs
  - Max: 95 µs
  - Mittelwert: 17 µs
- Server
  - Min: 1 µs
  - Max: 177 µs
  - Mittelwert: 27 µs

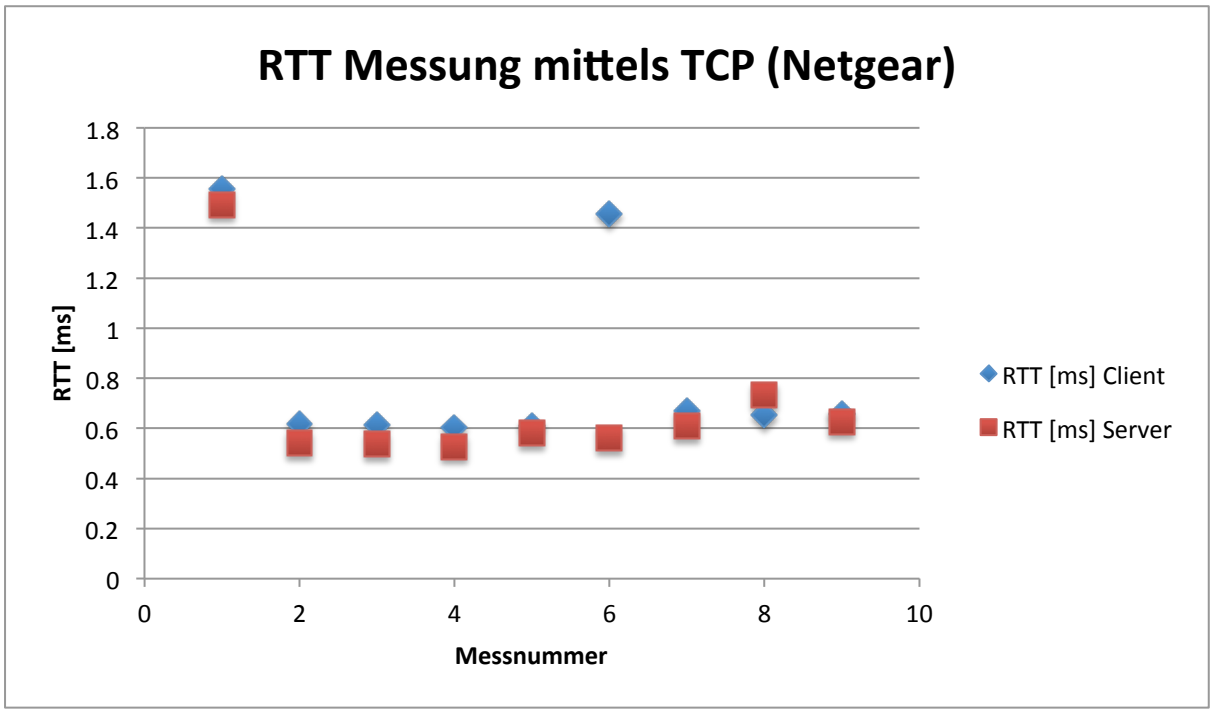
Beim Netgear Access Point ist zu erkennen, dass er im gestörten Umfeld einen deutlich tieferen RTT-Wert aufweist als der Cisco Access Point. Die Verarbeitungszeit beim Server bzw. Client hat sich nicht wesentlich verändert, sie kann somit nicht zu dieser Verkürzung der RTT geführt haben. Die Ursachen bleiben also unklar.

GESTÖRTES UMFELD



Im obigen Diagramm liegen die RTT-Werte für Server und Client ziemlich nahe beieinander und sind fast konstant. Trotzdem gibt es einzelne Ausreisser wie bei der Messnummer 4. Nach Analyse des Sniffer-Traces ist keine Anomalie zu erkennen. Das heisst, es wurde kein ARP-Request und ARP-Response gesendet. Vielmehr hängt die Abweichung wieder mit der Backoff-Zeit des Clients zu tun, der den Zugriff auf das Medium verzögerte.

HF-KAMMER



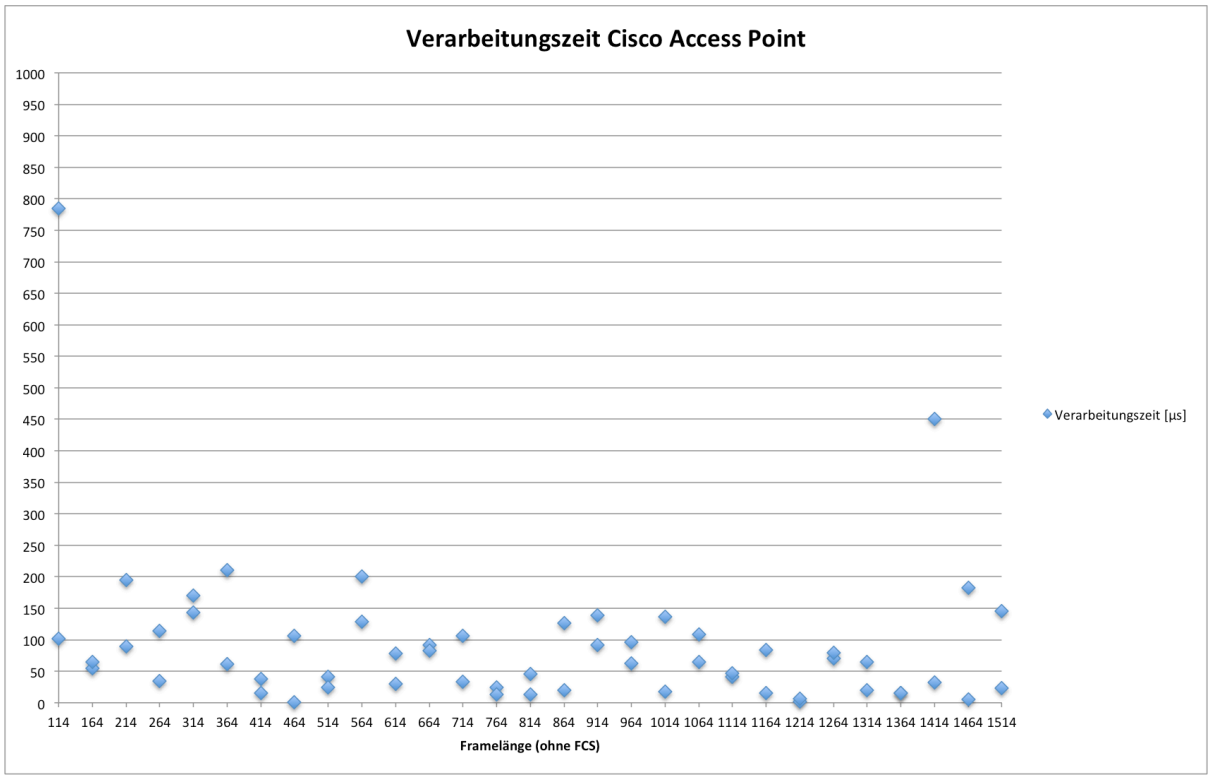
In der HF-Kammer sind die RTT-Werte sehr ähnlich wie jene im gestörten Umfeld. Bei der ersten Messung kam der Ausreisser wiederum dadurch zustande, dass der Server sich für die Kommunikation vorbereiten musste. Dazu gehört auch wieder die Reservierung eines Puffers über das Betriebssystem. Dies führt dann zu Verzögerungen auf Seiten des Servers. Wenn dann noch die anderen Verzögerungen, wie Zugriff auf das Medium, Serialisierungszeit und Konvertierungszeit beim Access Point, dazukommen, kann es durchaus sein, dass der erste RTT-Wert leicht höher ausfällt als die folgenden.

VERARBEITUNGSZEIT DER ACCESS POINTS

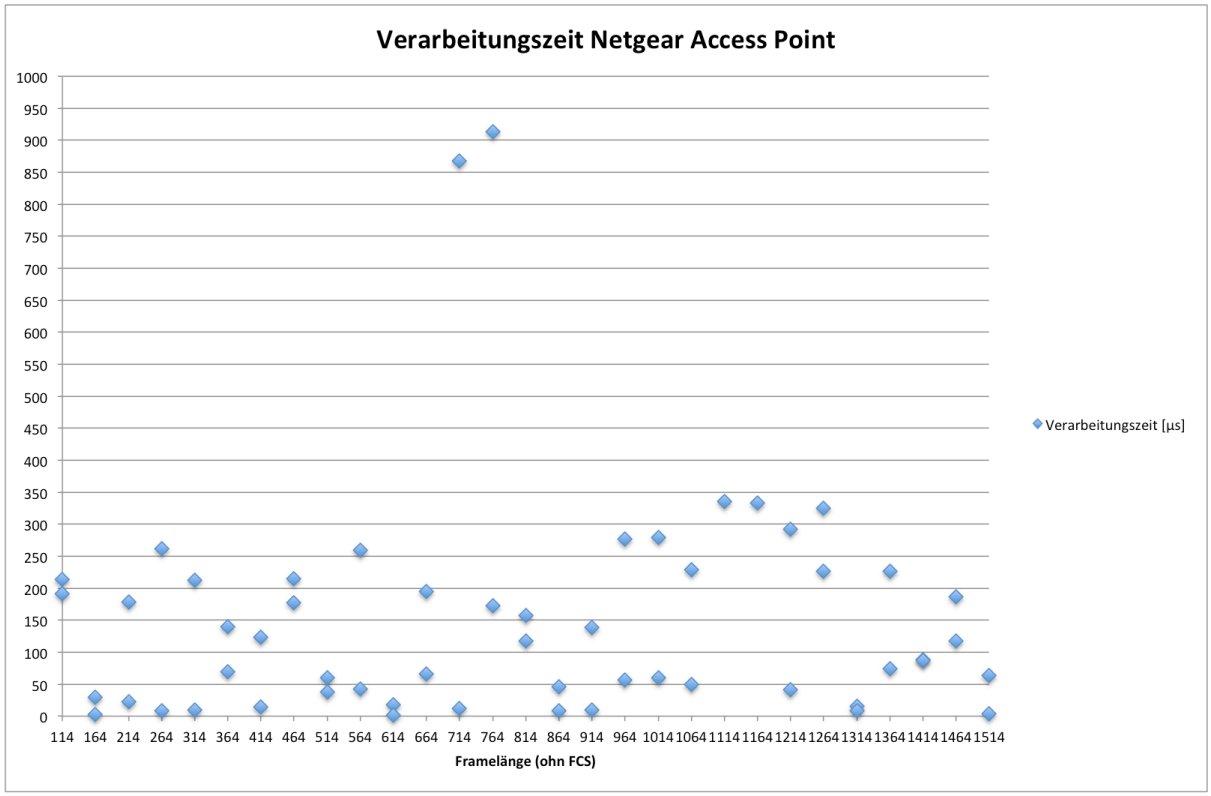
In den untenstehenden Diagrammen sind die Verarbeitungszeiten der verwendeten Access Points dargestellt. Gemessen wurde, wann ein Frame über die Luft übertragen wurde und wann es auf dem Ethernet-Medium sichtbar wurde. Die Subtraktion des erstgenannten Zeitwertes vom letzteren ergibt die Verarbeitungszeit. Die Zeitwerte wurden unter Verwendung des ICMP-Protokolls gemessen. Dabei wurden verschiedene Frame-Längen von 118 Byte bis 1518 Byte verwendet, in Abständen von 50 Byte. Diese Messungen wurden zweimal ausgeführt. Dabei wurde die Signallaufzeit nicht berücksichtigt, da die Distanzen zwischen den Notebooks und dem Access Point sehr kurz (max. 1m) waren. Beim Cisco Access Point liegen fast alle Werte unter 250 µs, beim Netgear Access Point unter 350 µs.

Bei den Messungen sind Schwankungen sichtbar. Hier ist es schwierig, eine Ursache zu benennen. Mögliche Gründe wären die Pufferzeiten (Lesen/Schreiben) des Switch und dass das Switching softwarebasiert, d.h. durch die CPU stattfindet.

CISCO



NETGEAR


Verarbeitungszeit Netgear Access Point
1000
950
900
850
800
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
0
114 164 214 264 314 364 414 464 514 564 614 664 714 764 814 864 914 964 1014 1064 1114 1164 1214 1264 1314 1364 1414 1464 1514
Framelänge (ohn FCS)
Verarbeitungszeit [µs]

G-STANDARD

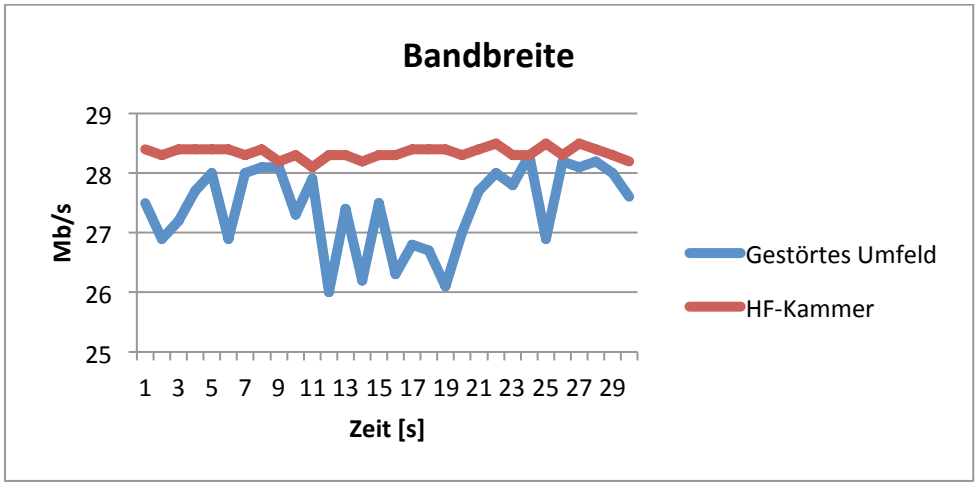
Bei den Messungen des G-Standards ist aus den Trace-Files ersichtlich, dass jedes Frame, welches vom Client zum Access Point gesendet wurde, von diesem mittels eines ACK-Frames bestätigt wurde. Dies führt dazu, dass pro gesendetes Frame zwei Zugriffe auf das Medium erforderlich sind. Erstens, um das Datenframe an den Access Point zu senden, und zweitens, um das ACK-Frame an den Client zu senden, sodass er die Information erhält, dass das Frame erfolgreich vom Access Point empfangen wurde. Bei den ACK-Frames war ersichtlich, dass diese fast immer sofort, also nach 1 µs, wieder ausgesendet worden sind. Dies liegt daran, dass die Access Points für ihre zu sendenden Daten kürzere Zugriffszeiten auf das Medium erhalten als die Stationen. Somit sind sie priorisiert beim Zugriff auf das Medium.

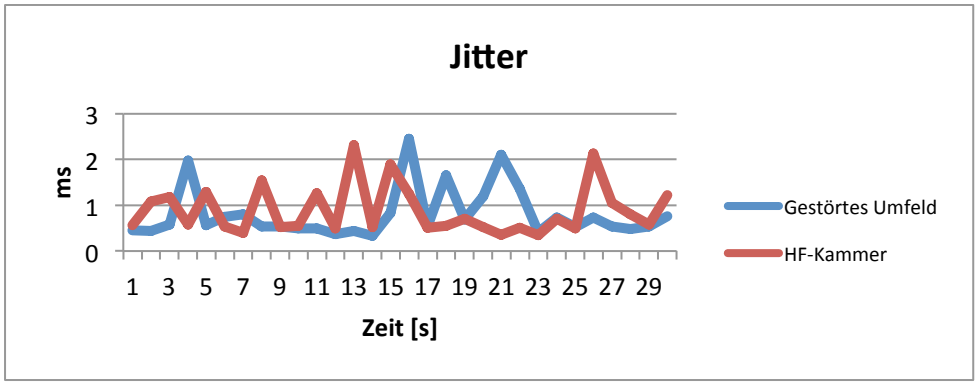
G (OHNE RTS/CTS)

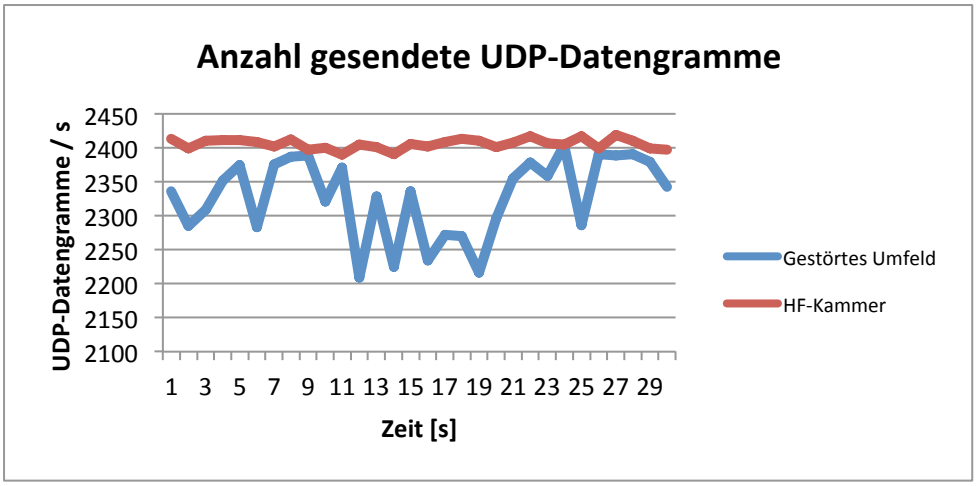
CISCO

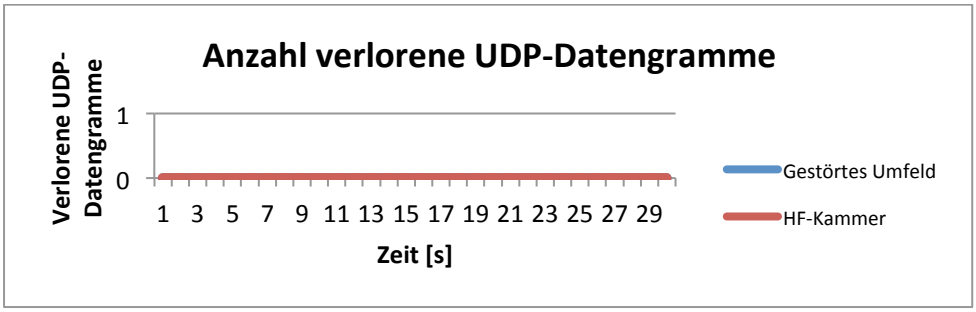
Bei der Messung des G-Standards ohne Verwendung des RTS-Mechanismus sendete der Client im Mittelwert alle 414 µs ein Frame aus. Der maximale Wert liegt bei 12 ms. Diese Frames werden dann vom Access-Point mit einem ACK-Frame bestätigt, wobei das ACK-Frame minimal eine Antwortzeit von 1 µs hat. Die maximale Dauer der Aussendung des ACK-Frames liegt bei 392 µs.

Der Cisco Access Point unterstützt im G-Standard nur die Short Preamble.









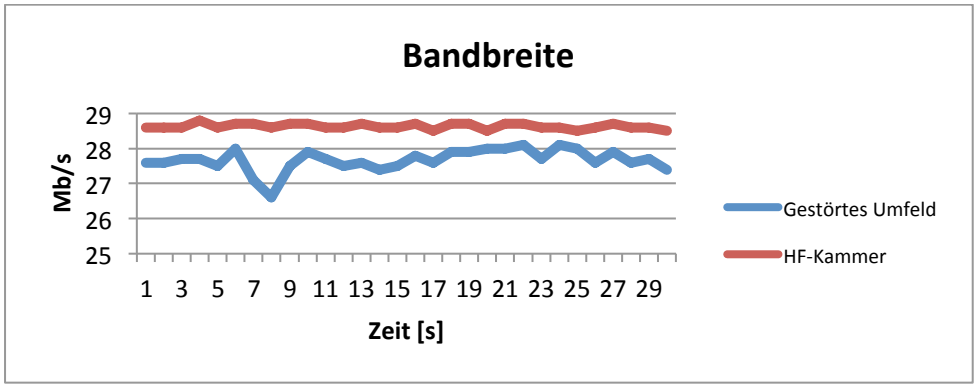
Beim Vergleich zwischen dem gestörten Umfeld und der HF-Kammer ist deutlich erkennbar, dass in der HF-Kammer die Bandbreite und die Anzahl gesendeter UDP-Datengramme sehr konstant sind. Die Anzahl der verlorenen UDP-Datengramme ist in beiden Umgebungen 0, sodass alle ausgesendeten Frames auch empfangen wurden.

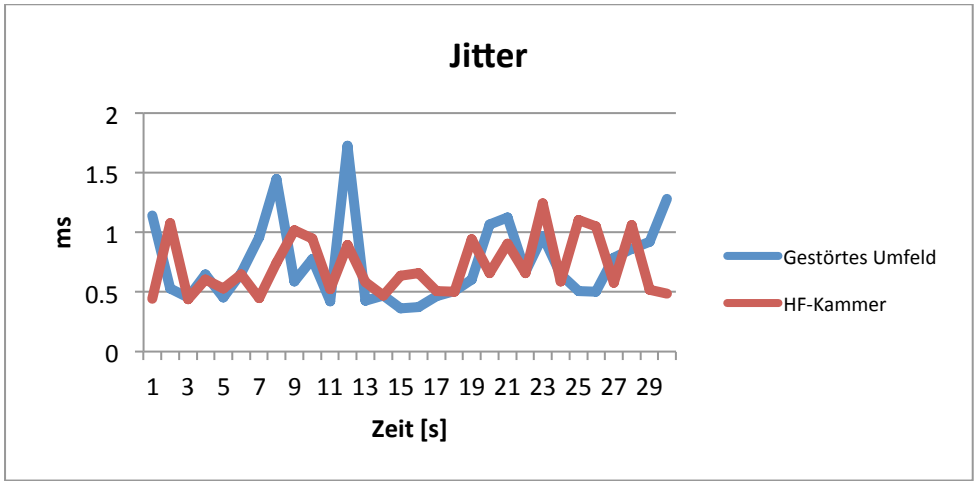
Hingegen sind in der gestörten Umgebung grosse Schwankungen aufgetreten. Vor allem ist in der Sekunde 12 ein Tief erreicht worden. Die Analyse der Trace-Files ergab, dass in diesem Bereich sehr viele Frames nicht durch ein ACK-Frame bestätigt worden sind und das ACK-Frame ein weiteres Mal gesendet werden musste. Daher musste der Sender mit dem Aussenden des nächsten Frames warten, bis er das ACK-Frame erfolgreich empfangen hatte. Dies führt dazu, dass er weniger Daten pro Sekunde senden kann, was sich dann auch wieder auf die Bandbreite auswirkt. Der Grund, warum sehr viele ACK-Frames zweimal ausgesendet werden mussten, waren sehr wahrscheinlich die Interferenzen von anderen vorhandenen WLANs. Dies würde auch erklären, warum ein solches Tief in der HF-Kammer nicht vorkam.

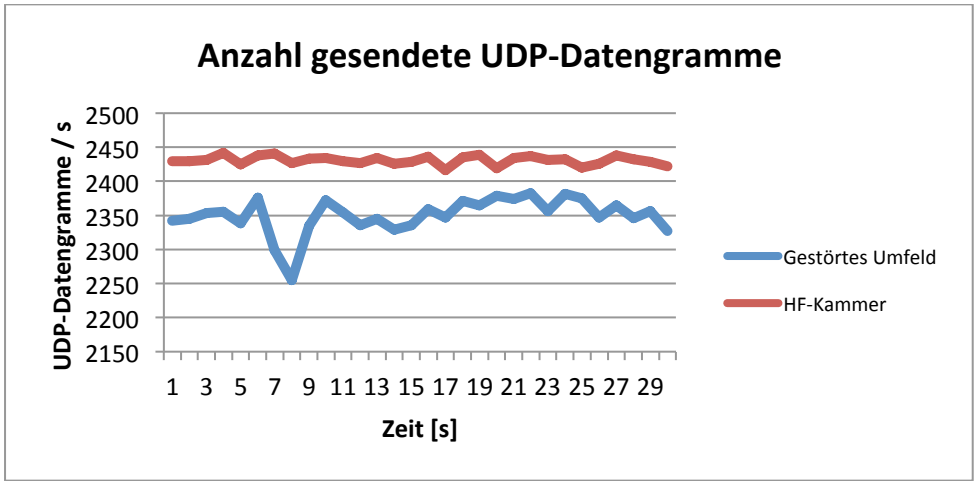
NETGEAR

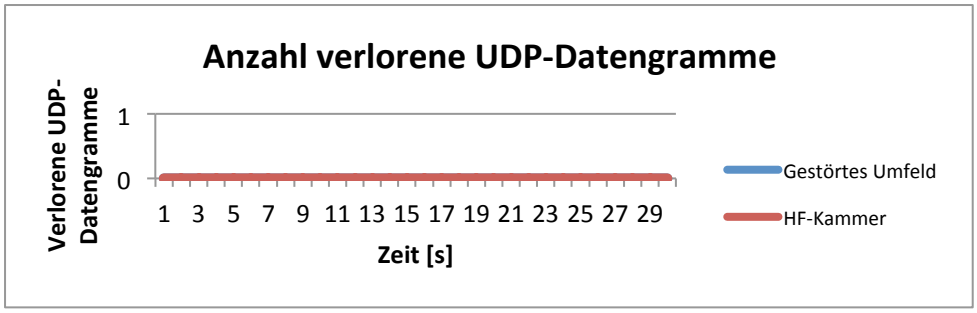
Der Client sendete bei den Messungen des G-Standards im Mittelwert alle 419 µs ein Frame aus. Der maximale Wert liegt bei 10,3 ms. Der Netgear Access Point sendet die ACK-Frames fast immer sofort nach ≤ 1 µs aus. Der maximale Wert liegt bei 6.14 ms. Die Backoff-Zeiten haben folgende Werte: CWmin: 15, CWmax: 1023.

SHORT PREAMBLE





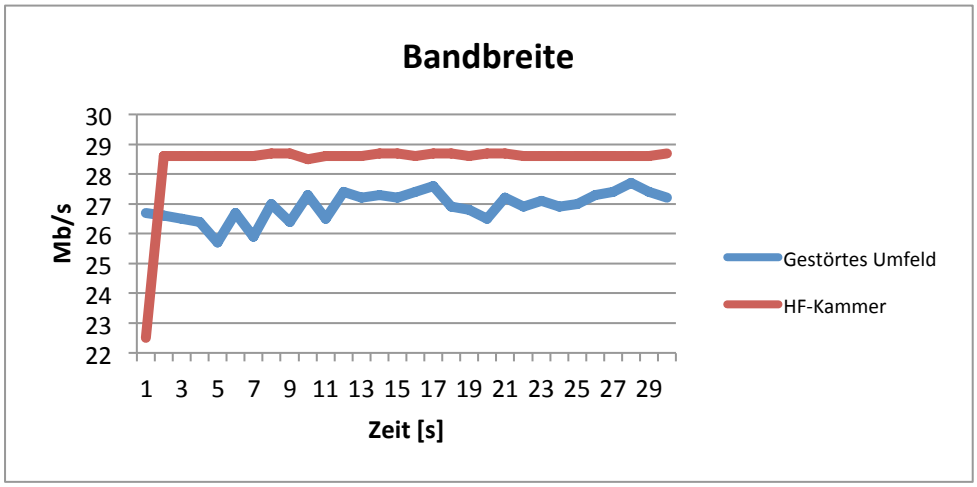


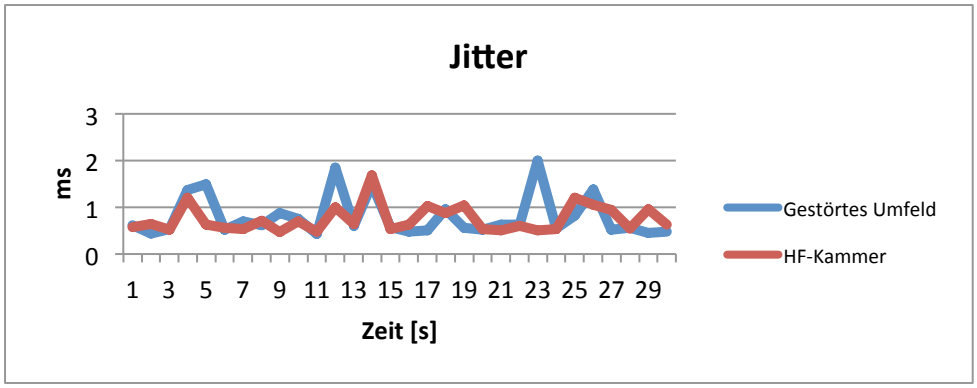


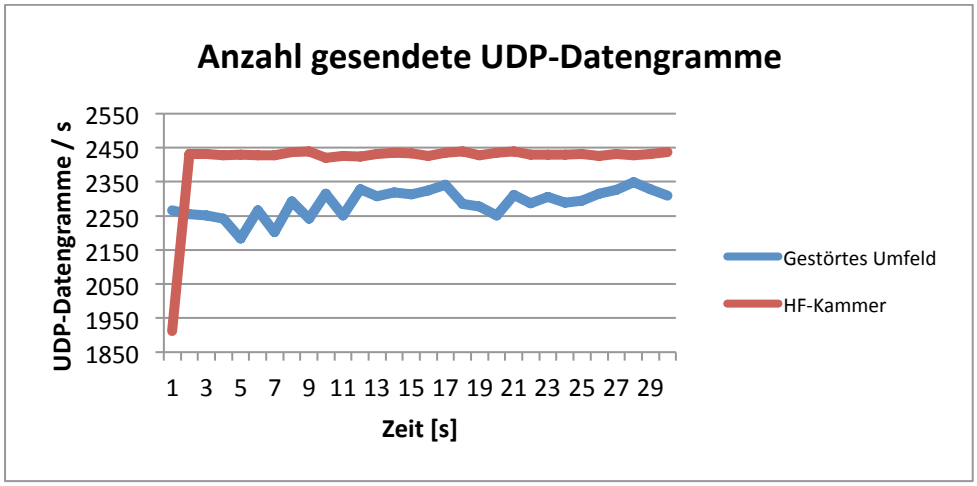
Vergleicht man die Messungen in der HF-Kammer mit denen vom Cisco Access Point, so ist erkennbar, dass bei etwa 28.5 Mbps der maximale Durchsatz des G-Standards erreicht worden ist. Dies liegt daran, dass jedes Frame einzeln bestätigt werden muss und deshalb pro gesendetes Frame zwei Medienzugriffe notwendig sind. Somit resultiert im optimalen Umfeld eine Nettobandbreite von 50 % der Bruttobandbreite.

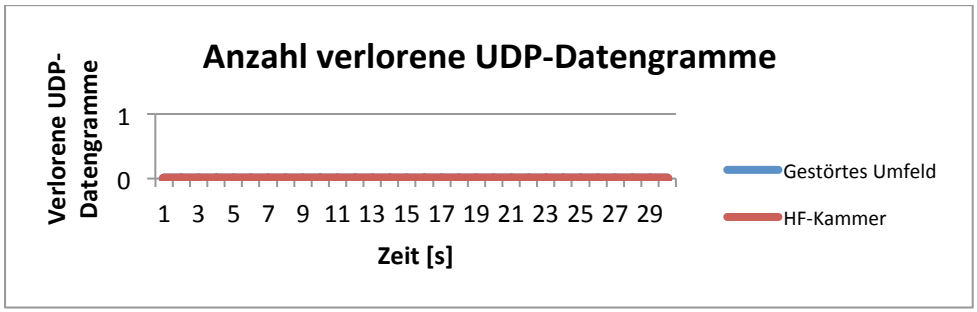
Im gestörten Umfeld ist wiederum die Auswirkung von Interferenzen zu erkennen. Die Bandbreite liegt im gestörten Umfeld immer deutlich unterhalb der Bandbreite in der HF-Kammer. Was den tiefsten Wert der Bandbreite und der Anzahl gesendete UDP-Datengramme betrifft, konnte festgestellt werden, dass ACK-Frames zweimal vom Access Point ausgesendet wurden. Das deutet darauf hin, dass diese ACK-Frames aufgrund von vorhandenen Interferenzen vom Client erst beim zweiten Mal empfangen wurden.

LONG PREAMBLE









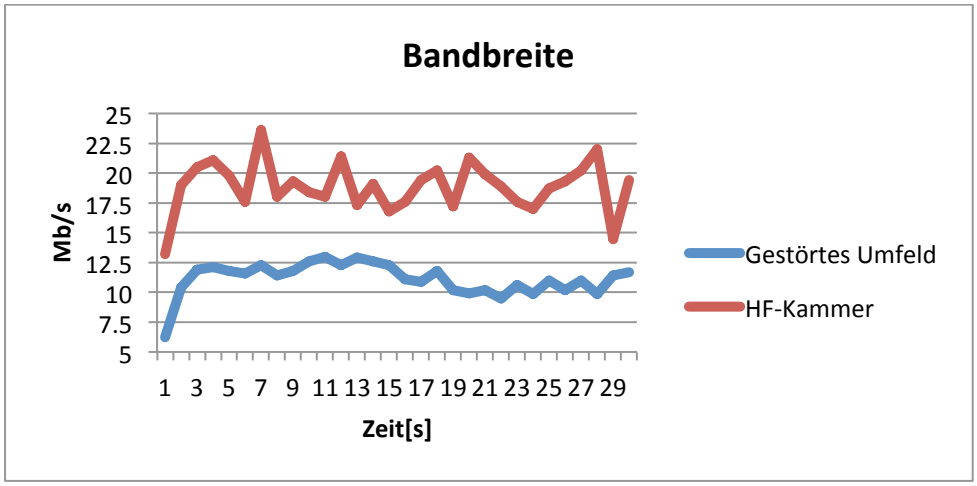
Die Verwendung des Long-Guard-Intervalls weist keine wesentlichen Unterschiede zur Verwendung des Short-Guard-Intervalls auf. In der gestörten Umgebung macht sich das Long-Guard-Intervall jedoch bemerkbar. Der einzige Unterschied ist, dass in der gestörten Umgebung Interferenzen vorhanden sind und dass daher nicht immer auf das Medium zugegriffen werden kann. Dies würde erklären, warum im gestörten Umfeld weniger UDP-Datengramme pro Sekunde übertragen werden können. Dadurch verzögert sich beim Sender der Zugriff auf das Medium. Wenn man dann noch die Zeit der Long Preamble mit einer Dauer von 72 µs pro ausgesendetes Frame dazuzählt, ist es verständlich, dass hier eine Verzögerung bei der Übertragung von Frames auftritt.

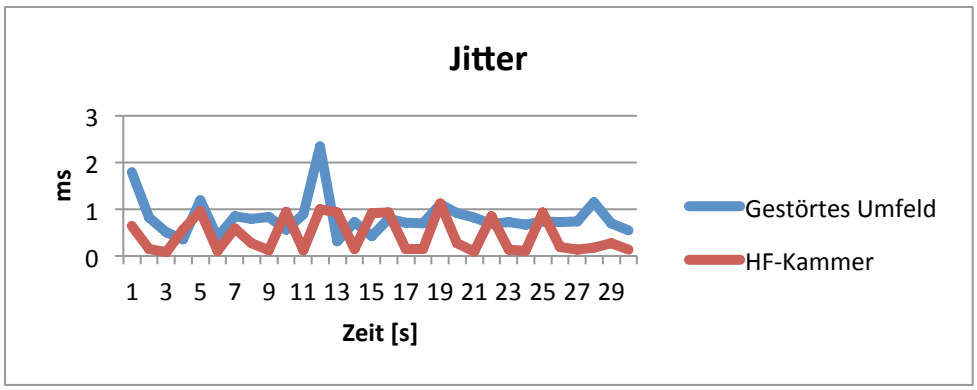
G (MIT RTS/CTS)

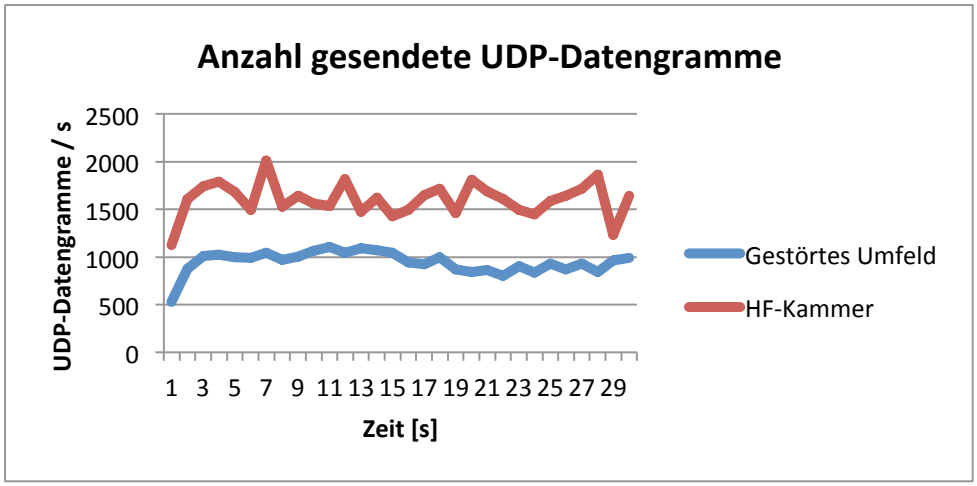
Mit dem RTS/CTS-Verfahren muss vor jedem Frame, welches ausgesendet wird, ein Request-to-Send-Frame vom Sender zum Empfänger gesendet werden. Ist das Medium frei, so sendet der Empfänger ein Clear-to-Send-Frame an den Sender zurück. Danach kann der Sender das Frame auf das Medium übertragen. Zusätzlich wird dann das erhaltene Frame vom Empfänger bestätigt. Bei diesem Mechanismus sind also pro gesendetes Frame insgesamt vier Zugriffe auf das Medium notwendig. Dies führt dazu, dass weniger Frames pro Sekunde gesendet werden können, was sich auf die Datenübertragungsrate auswirkt. Da ein Access Point beim Medienzugriff privilegiert ist und sofort ein Frame aussenden kann unter der Voraussetzung, dass das Medium frei ist, kann er auf ein RTS-Frame sofort ein CTS-Frame zurücksenden. Somit muss als Resultat mit mindestens einer Halbierung des Durchsatzes gerechnet werden, wenn RTS/CTS verwendet wird.

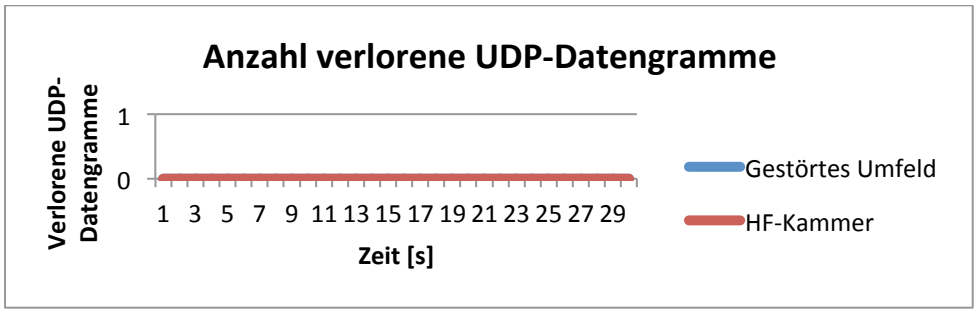
CISCO

Bei der Messung des G-Standards mit Verwendung des RTS/CTS-Mechanismus sendete der Client im Mittelwert alle 442 µs ein Frame aus. Der maximale Wert liegt bei 12 ms. Diese Frames werden dann vom Access Point mit einem ACK-Frame bestätigt, wobei dieses eine Antwortzeit von mindestens 1 µs hat.

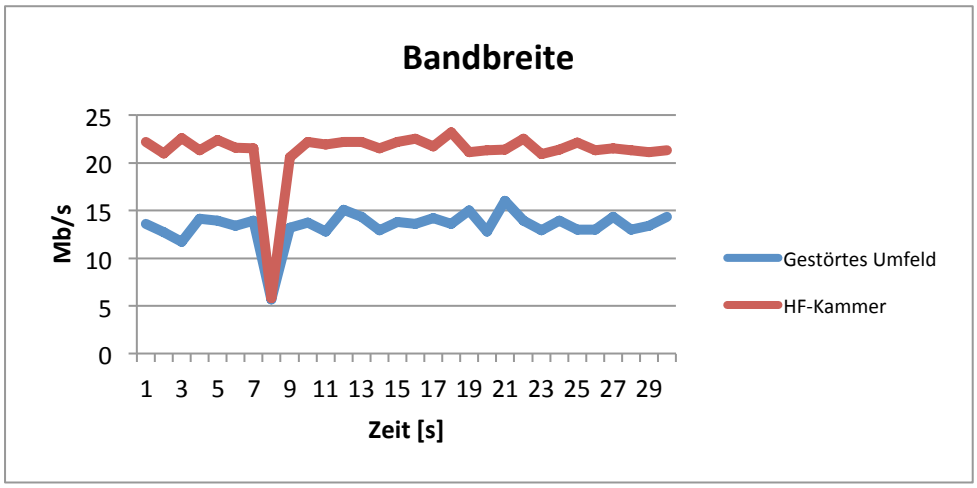


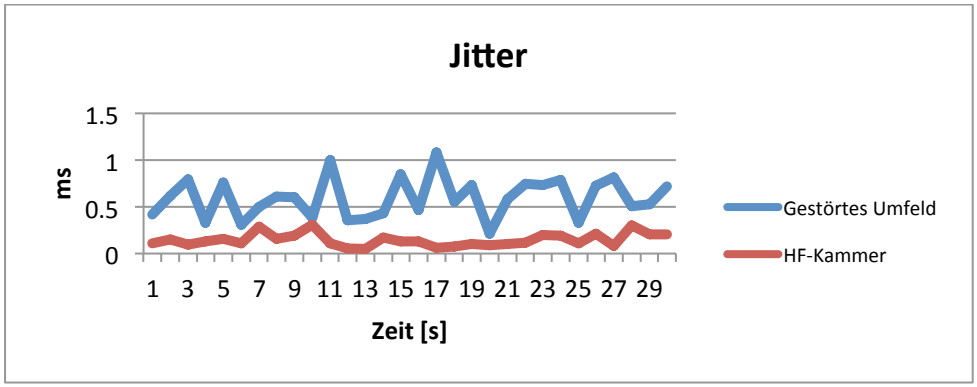


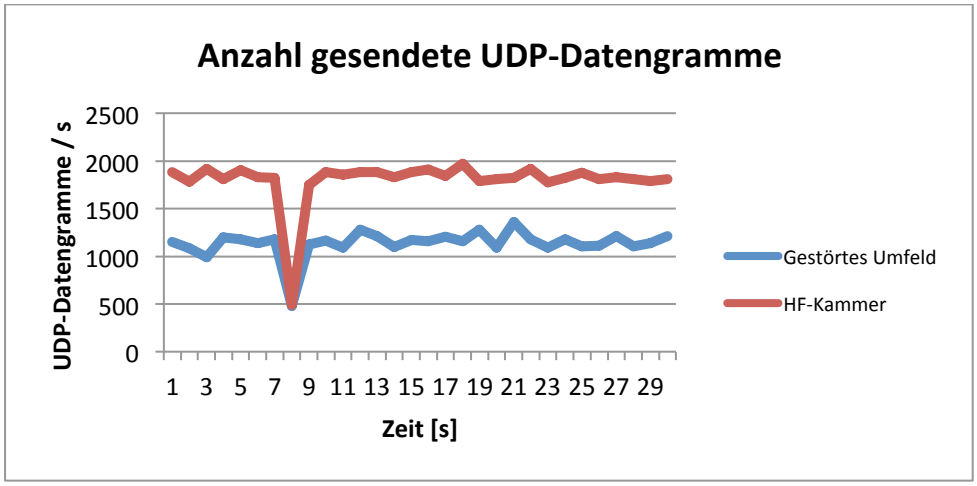


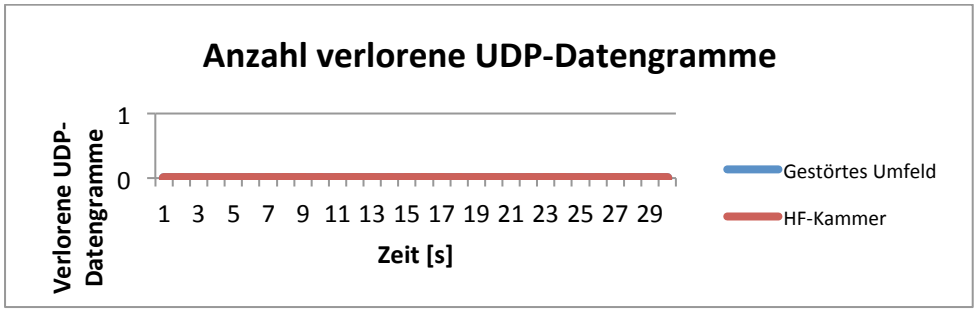


Beim G-Standard unter Verwendung des RTS/CTS-Mechanismus ist deutlich erkennbar, dass der Durchsatz im gestörten Umfeld im Vergleich zur Situation ohne Verwendung des RTS/CTS-Mechanismus mehr als halbiert worden ist. Wie zu erwarten war, ist die Anzahl der gesendeten UDP-Datengramme pro Sekunde sehr stark gesunken. Dies liegt daran, dass für das Aussenden eines UDP-Datengrammes vier Zugriffe auf das Medium notwendig sind.


Bandbreite
Mb/s
25
20
15
10
5
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer


Jitter
ms
1.5
1
0.5
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer


Anzahl gesendete UDP-Datengramme
UDP-Datengramme / s
2500
2000
1500
1000
500
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer


Anzahl verlorene UDP-Datengramme
Verlorene UDP-Datengramme
1
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

Bei den Messungen mit aktiviertem RTS/CTS-Mechanismus ist wiederum erkennbar, dass im gestörten Umfeld die Bandbreite zwischen 11 und 16 Mbps liegt. Da beim RTS/CTS-Mechanismus vier Medienzugriffe benötigt werden, um ein einzelnes Datenframe zu übertragen, können weniger Datenframes pro Sekunde übertragen werden. In der HF-Kammer liegt die Bandbreite zwischen 21 und 23 Mbps. Ein Grund für die Tatsache, dass die Bandbreite in der HF-Kammer höher ist, sind die Interferenzen.

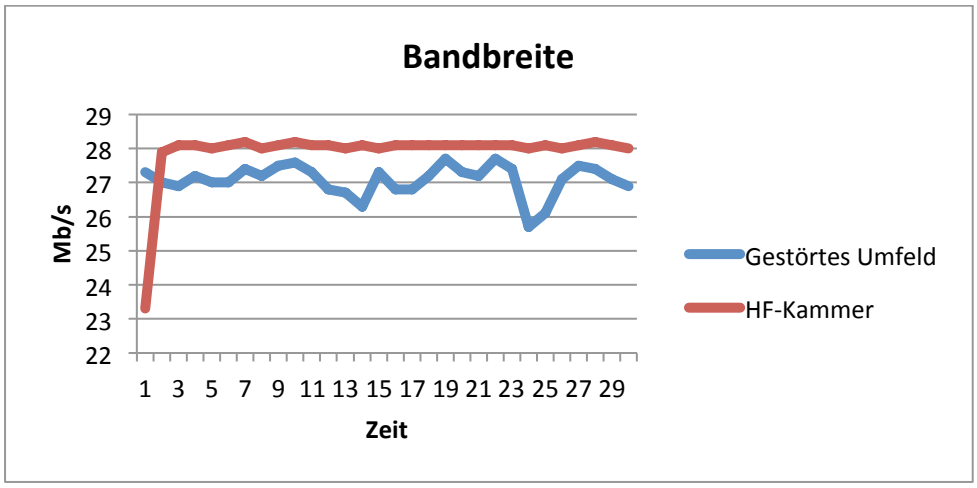
Bei beiden Messungen ist bei Sekunde 8 ein deutlicher Einbruch auf 5.81 Mbps zu erkennen. Warum dieser Einbruch aufgetreten ist, kann aufgrund der Trace-Files nicht nachvollzogen werden.

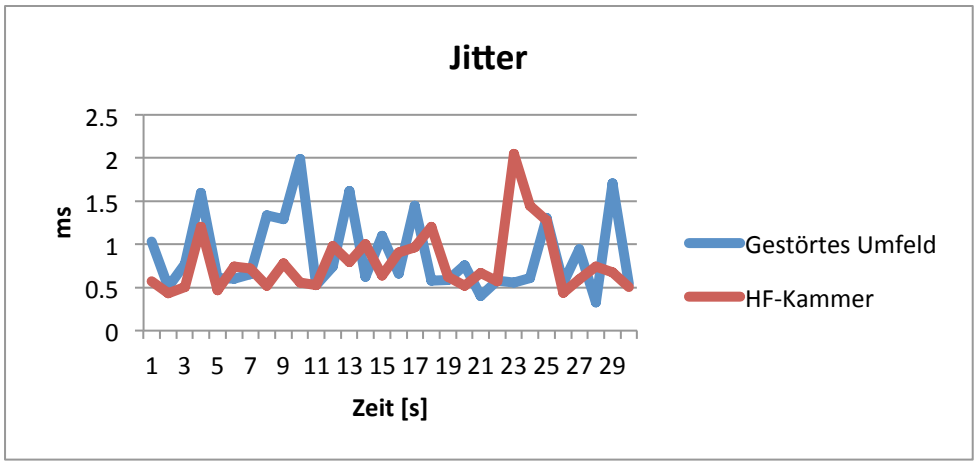
E-STANDARD

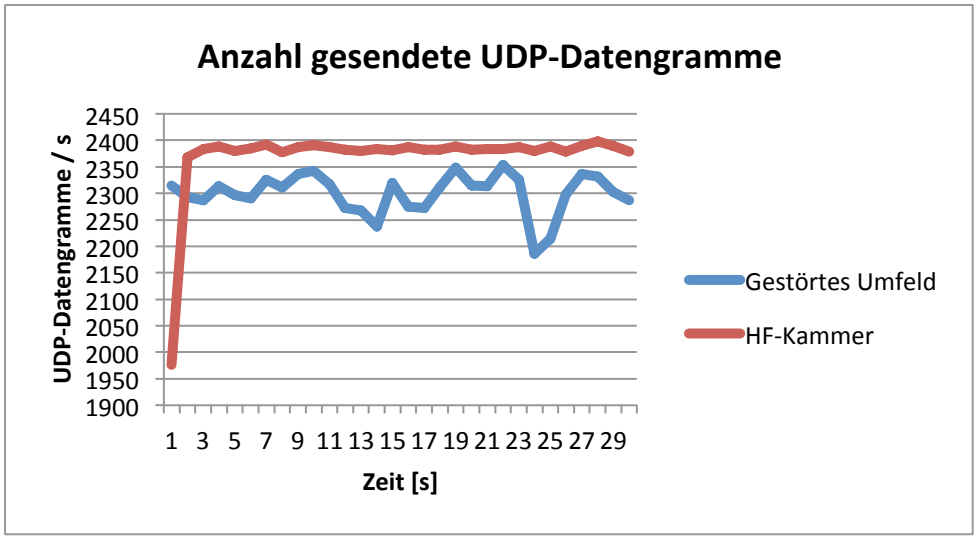
Bei der Messauswertung des E-Standards fiel auf, dass beide Access Points diesen Standard nicht voll implementiert haben. Dabei unterstützt weder der Cisco noch der Netgear Access Point die Verwendung des Block-Acknowledgements. Dies hat zur Folge, dass jedes einzelne Frame vom Empfänger bestätigt werden muss, bevor der Sender das nächste Frame übertragen darf. Beim Cisco Access Point gab es keine Möglichkeit, manuell die AIFS-Werte anzupassen. Der Netgear Access Point erlaubt es, diese AIFS-Werte inklusive TXOP-Limit, CWmin- und CWmax-Werte manuell einzustellen.

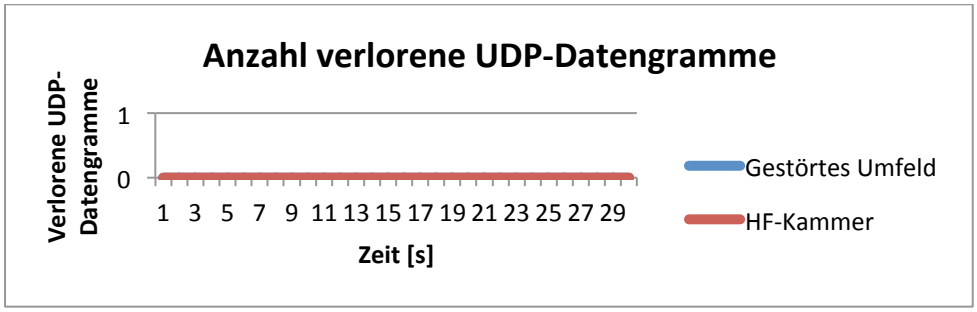
CISCO

Bei der Messung des E-Standards sendete der Client im Mittelwert alle 429 µs ein Frame aus. Der maximale Wert liegt bei 10 ms. Diese Frames werden dann vom Access Point mit einem ACK-Frame bestätigt, welches minimal eine Antwortzeit von 1 µs hat. Die maximale Aussendedauer des ACK-Frames liegt bei 414 µs.







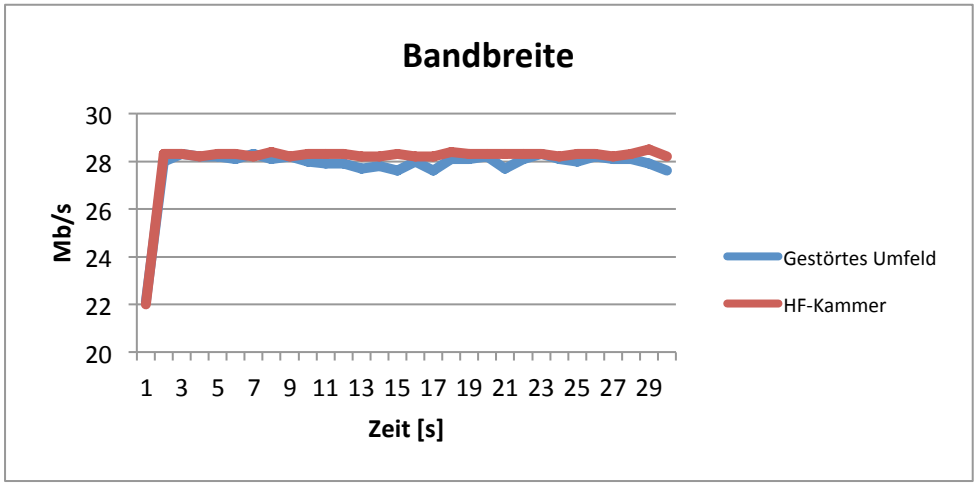


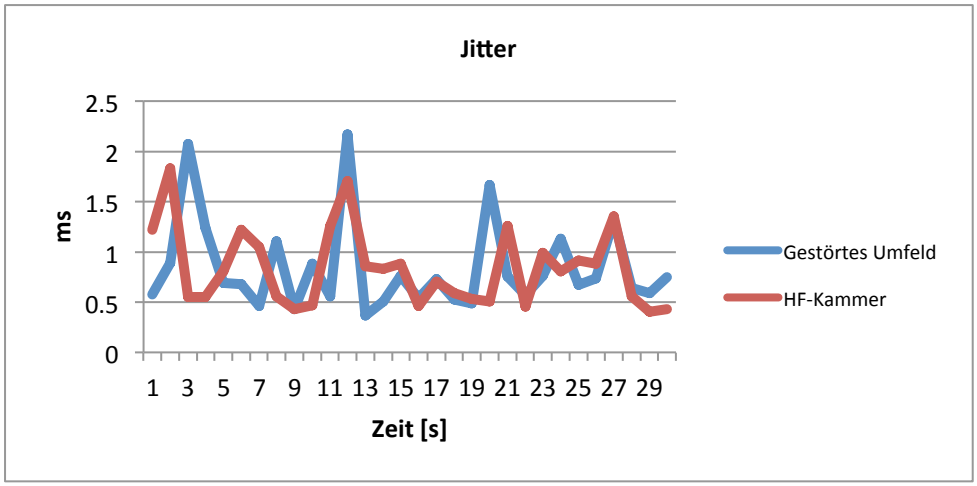
Die Werte in der HF-Kammer sind nach der ersten Sekunde sehr konstant. Es wird in etwa immer dieselbe Anzahl von UDP-Datengrammen pro Sekunde gesendet. Dies bedeutet wiederum, dass auch die Bandbreite konstant ist.

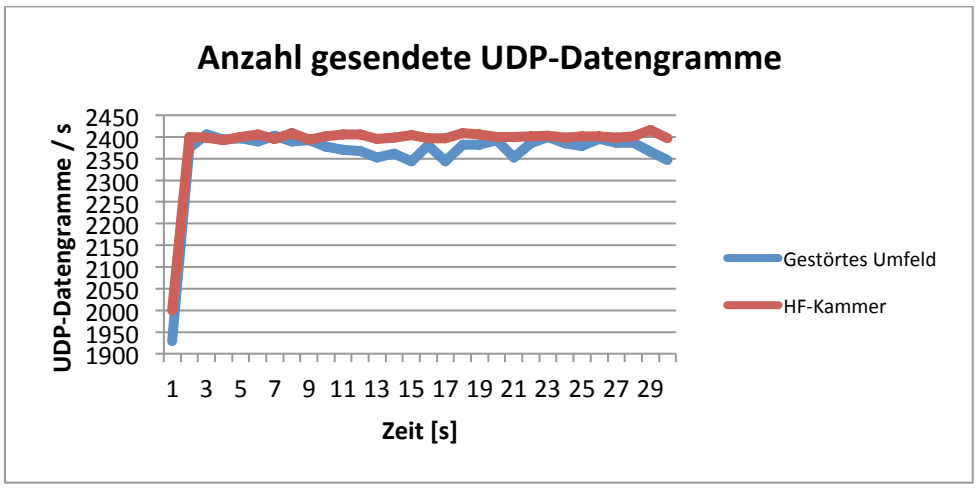
Im Vergleich zu den Messungen des G-Standards ohne RTS/CTS ist keine Verbesserung des Durchsatzes ersichtlich.

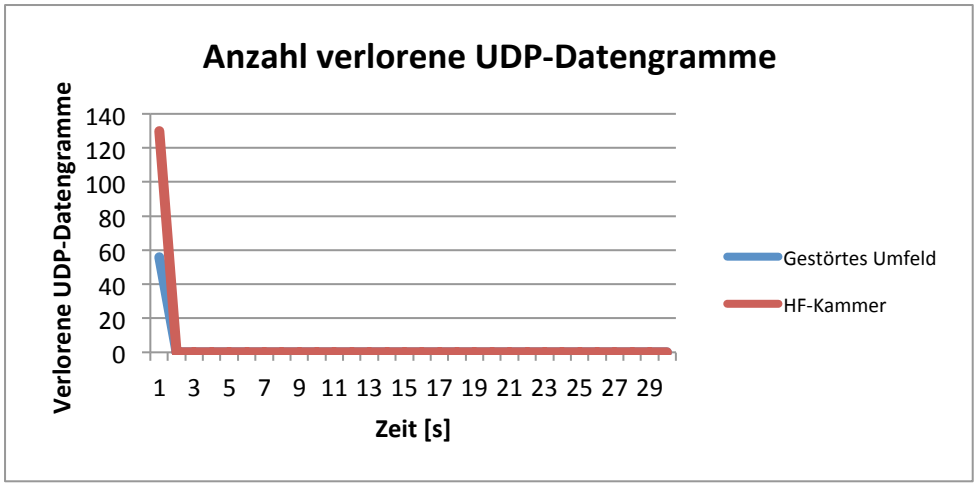
NETGEAR

E (BEST EFFORT)







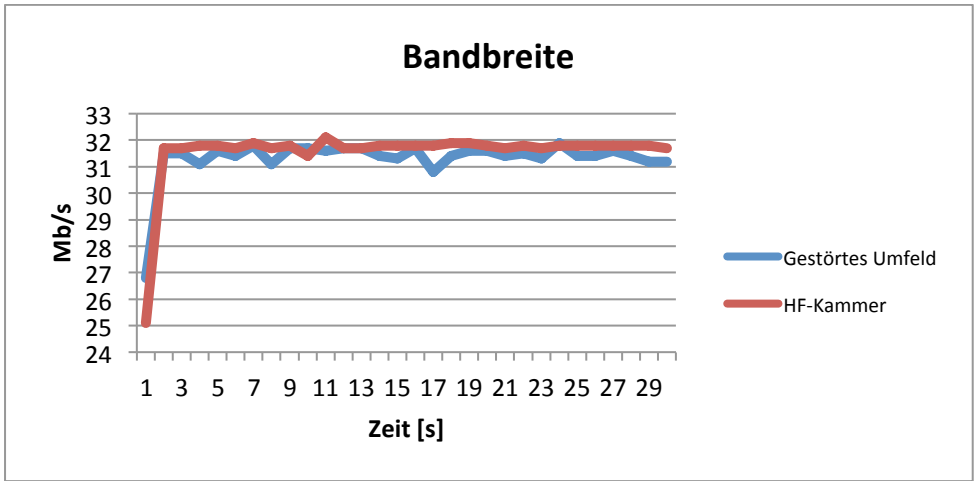


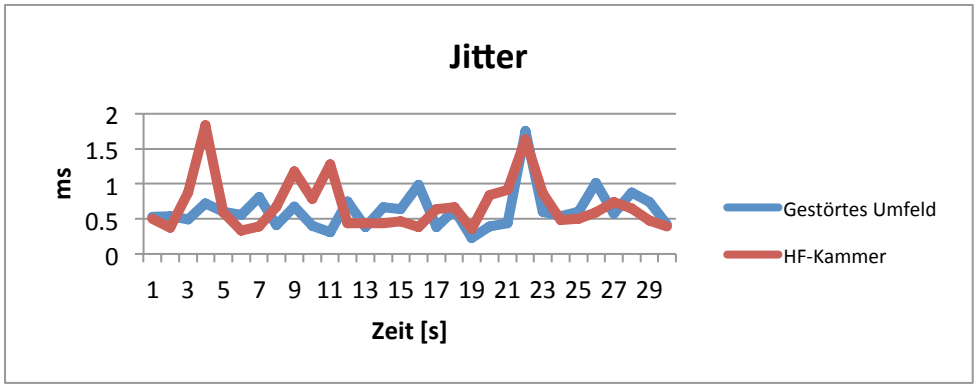
Nach der Aktivierung des E-Standards beim Netgear Access Point wurden die Parameter wie folgt eingestellt: AIFS 3, CWmin 15, CWmax 63. Im Vergleich zum G-Standard ist nur der CWmax kleiner geworden.

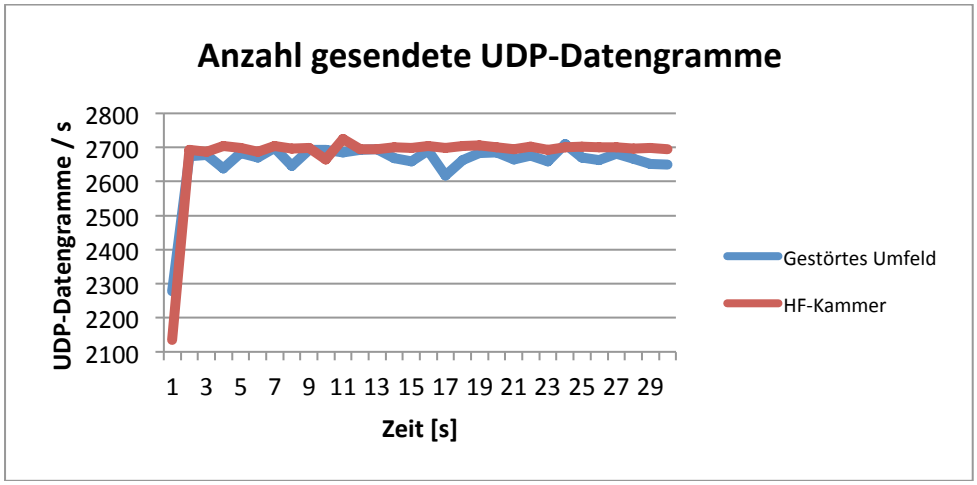
Aus diesen Messungen wird ersichtlich, dass im ungestörten Umfeld die Bandbreite leicht konstanter ausfällt als ohne aktivierten E-Standard. In der HF-Kammer ist eher ein leicht tieferer Wert festzustellen. Dass hier keine Verbesserung des Durchsatzes erzielt wurde, liegt unter anderem daran, dass der Verkehr, der bei den Messungen generiert wird, vom Access Point als „Best Effort“ behandelt wird. Diese Verkehrsklasse hat die zweittiefste Priorität. Der AIFS mit der Nummer 3 ergibt somit wieder die Zugriffszeit auf das Medium, wie sie schon im G-Standard verwendet worden ist. Der einzige Unterschied zwischen dem G- und dem E-Standard sind deshalb die CWmax-Werte. Obwohl diese Werte verschieden sind, ist die erreichte Bandbreite dieselbe. Daraus lässt sich schliessen, dass in den Messungen des G-Standards nie das CWmax erreicht worden ist.

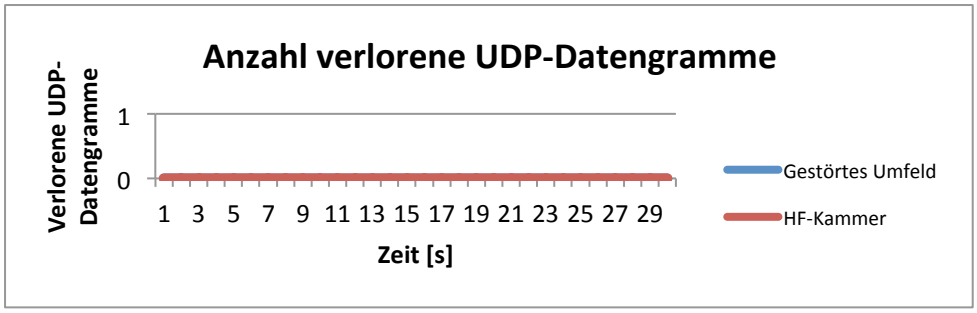
E (VIDEO)

Bei dieser Messung wurde der gesendete Verkehr als Video-Verkehr simuliert. Dabei wurde die „Best Effort Queue“ des Netgear Access Point mit folgenden Backoff-Parametern eingestellt: AIFS 2, CWmin 7, CWmax 15. Das TXOP-Limit ist auf 3008 gesetzt. Aufgrund dieser Parameter ist eine Steigerung der Anzahl UDP-Datengramme pro Sekunde zu erwarten, weil mit diesen Einstellungen die Zugriffszeiten auf ein freies Medium verkürzt worden sind.







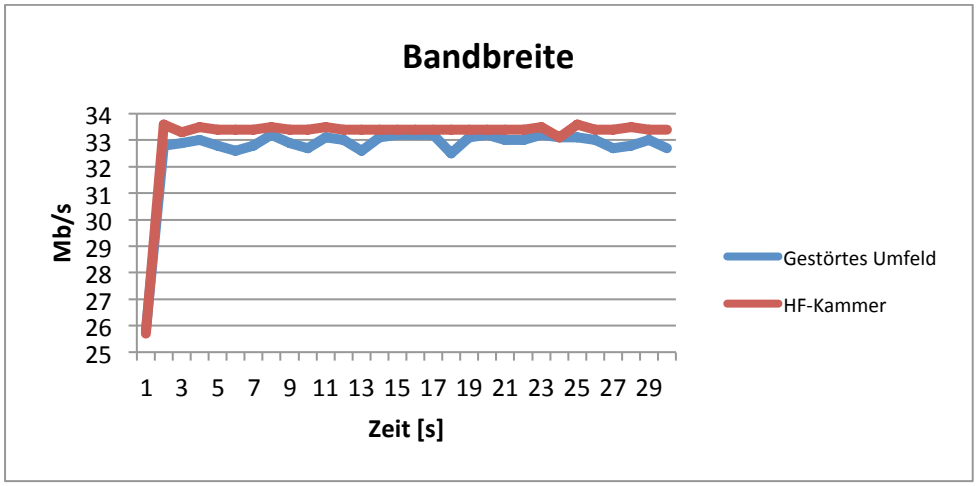


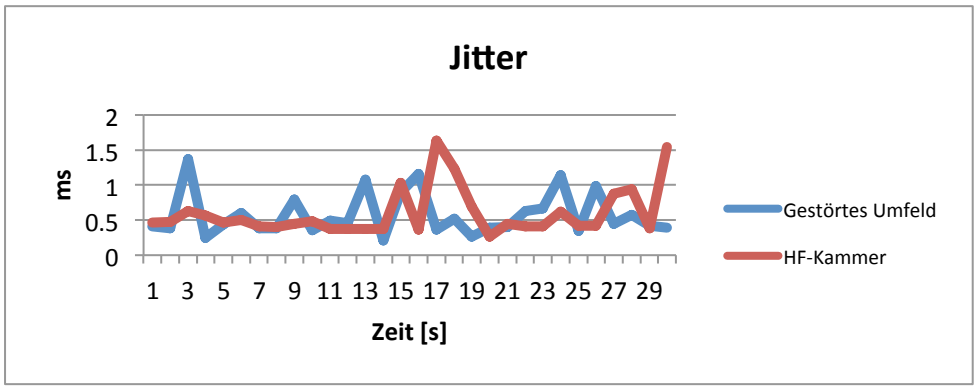
Wie erwartet, ist die Anzahl gesendeter UDP-Datengramme gestiegen. Daher ist auch die Bandbreite markant angestiegen, im Vergleich zum G-Standard um ganze vier Mbps. Daraus ist erkennbar, welchen Einfluss die Medienzugriffszeit auf den Durchsatz von WLANs hat. Mit einem besseren Zugriffsverfahren kann eine Steigerung des Durchsatzes um ca. 20 % erreicht werden.

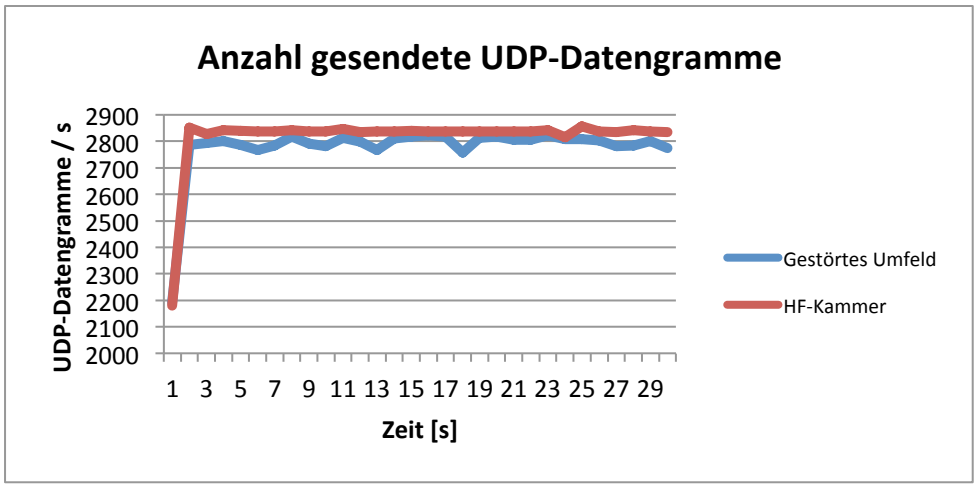
Mithilfe dieses Wissens kann nun bei vorhandenen Installationen je nach Bedarf die Bandbreite erhöht werden. Vor allem in Heimnetzwerken liesse sich so die Bandbreite noch einmal erhöhen, indem die Backoff-Parameter tiefer eingestellt werden.

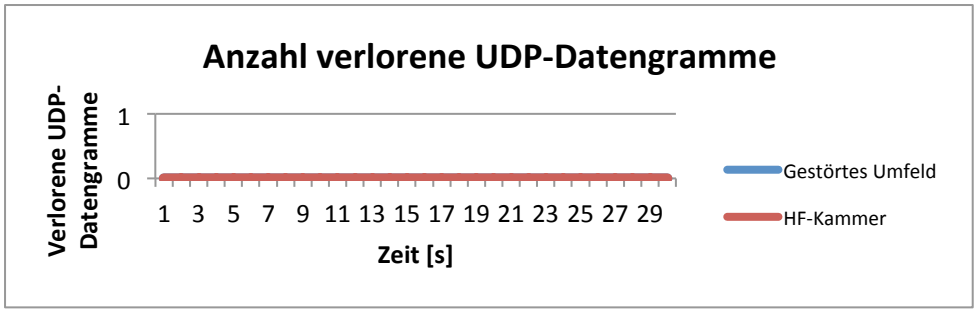
E (VOICE)

Bei dieser Messung wurde der gesendete Verkehr als Voice-Verkehr simuliert. Dabei wurde die „Best Effort Queue“ des Netgear Access Point mit folgenden Backoff-Parametern eingestellt: AIFS 2, CWmin 3, CWmax 7. Das TXOP-Limit ist auf 1504 gesetzt. Durch Anpassung dieser Parameter ist eine weiter Steigerung der Anzahl UDP-Datengramme pro Sekunde zu erwarten, weil so die Zugriffszeiten auf ein freies Medium nochmals verkürzt worden sind.









Auch hier ist wieder zu erkennen, dass die Zugriffszeit auf das Medium einen wesentlichen Einfluss auf den Durchsatz von WLANs hat. Durch die kürzere Zugriffszeit kann eine grössere Anzahl an Frames pro Sekunde ausgesendet werden. Durch weitere Anpassung der oben beschriebenen Parameter ist der Durchsatz um weitere zwei Mbps gestiegen. Im Vergleich zum G-Standard ist der Durchsatz somit um vier Mbps höher. Das entspricht einer Steigerung um rund 25 %.

Aufgrund dieser Messungen kann die Aussage gemacht werden, dass nicht nur Interferenzen einen enormen Einfluss auf den Durchsatz von WLANs haben, sondern auch die Zugriffszeiten auf das Medium.

N-STANDARD

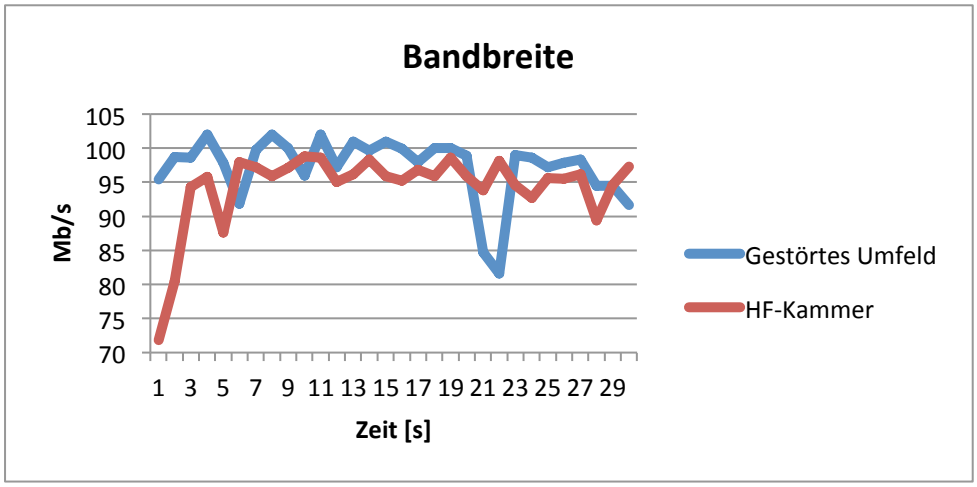
Beim Cisco Access Point gibt es keine Möglichkeit, die Aggregation von Frames zu deaktivieren. Deshalb ist die Aggregation von Frames bei allen durchgeführten Tests aktiviert. Wenn die Aggregation verwendet wird, kommt auch der Compressed-Block-Acknowledge-Mechanismus zum Einsatz. Des Weiteren ist die Verwendung von RIFS bei Cisco automatisch erlaubt.

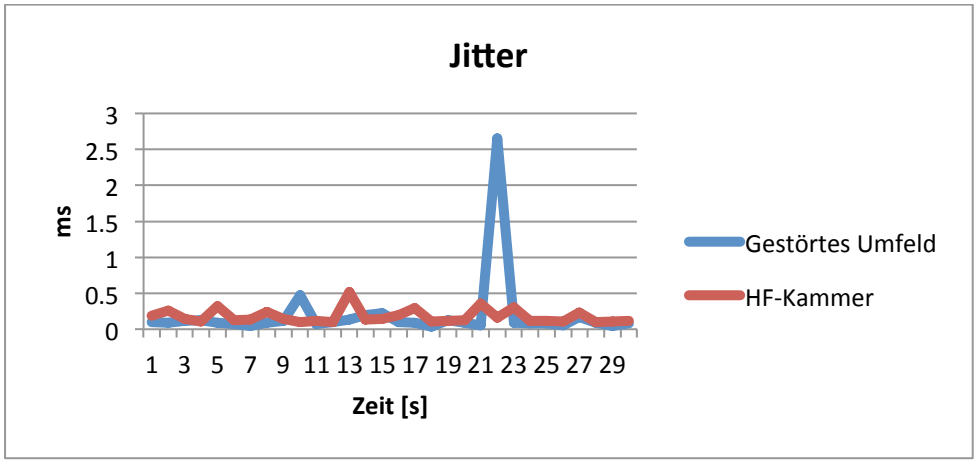
Bei den Messungen des N-Standards fällt auf, dass bei manchen Messungen die erreichte Bandbreite in der HF-Kammer geringer ist als im gestörten Umfeld. Der Grund dafür liegt in der Verwendung von MIMO-Antennen. Hierbei werden die Signale über mehrere Antennen ausgesendet und an Wänden und Gegenständen unterschiedlich reflektiert, bis sie das Ziel erreichen. Weil in der HF-Kammer die Signale an den Wänden absorbiert werden, funktioniert diese Technologie nicht einwandfrei. Das führt dann zu einer geringeren Bandbreite und zum Verlust bzw. erneuten Aussenden von UDP-Datengrammen.

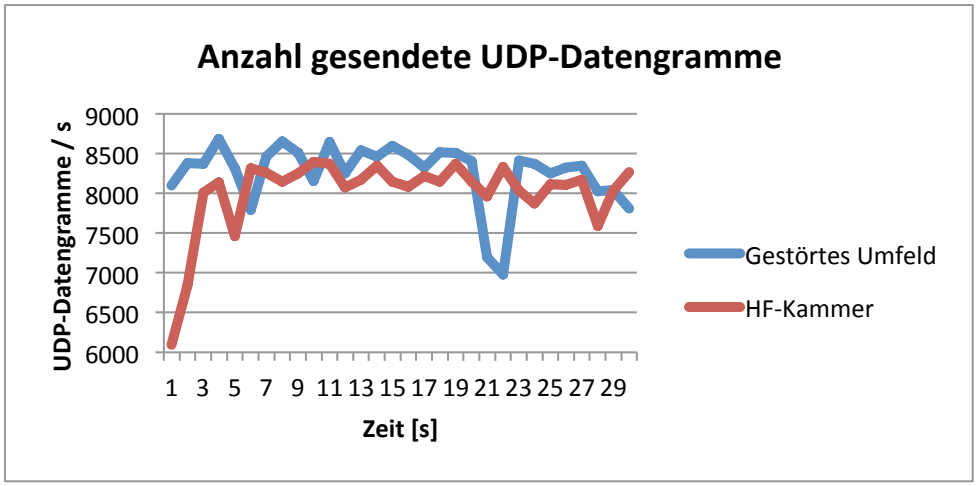
2.4-GHZ-FREQUENZBAND

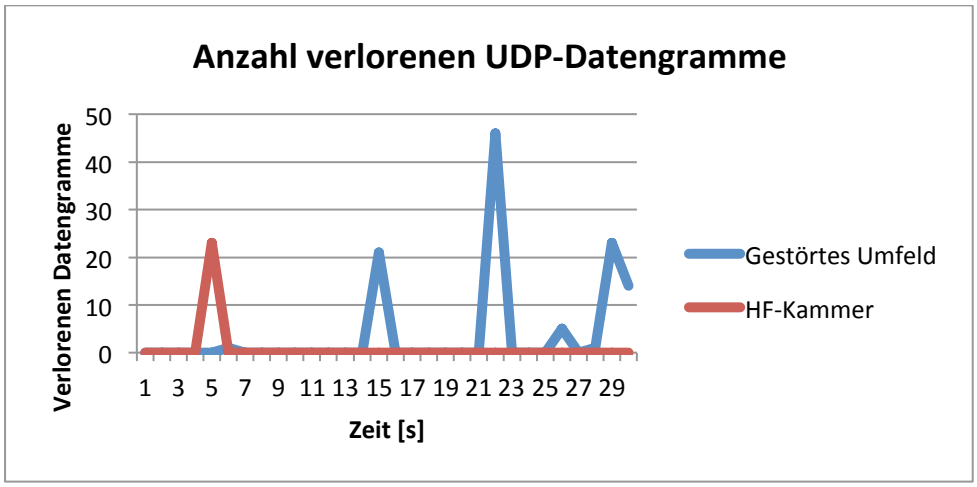
SHORT GUARD, 20 MHZ KANALBREITE

CISCO









In den obigen Diagrammen fällt auf, dass in den ersten drei Sekunden der Messung in der HF-Kammer ein sehr geringer Durchsatz erreicht wurde. Dies widerspiegelt sich auch in der Tatsache, dass während dieser Zeit eine vergleichsweise geringe Anzahl UDP-Datengramme pro Sekunde übertragen wurde. Dabei wurde in den Trace-Files ersichtlich, dass in den ersten 200 Millisekunden keine Aggregation von Frames verwendet worden ist. Nach den 200 Millisekunden wird die Aggregation von Frames aktiviert. Dies hat einen wesentlichen Einfluss darauf, wie viele UDP-Datengramme pro Sekunde übertragen werden können. Das erklärt, warum zu Beginn weniger UDP-Datengramme pro Sekunde übertragen wurden.

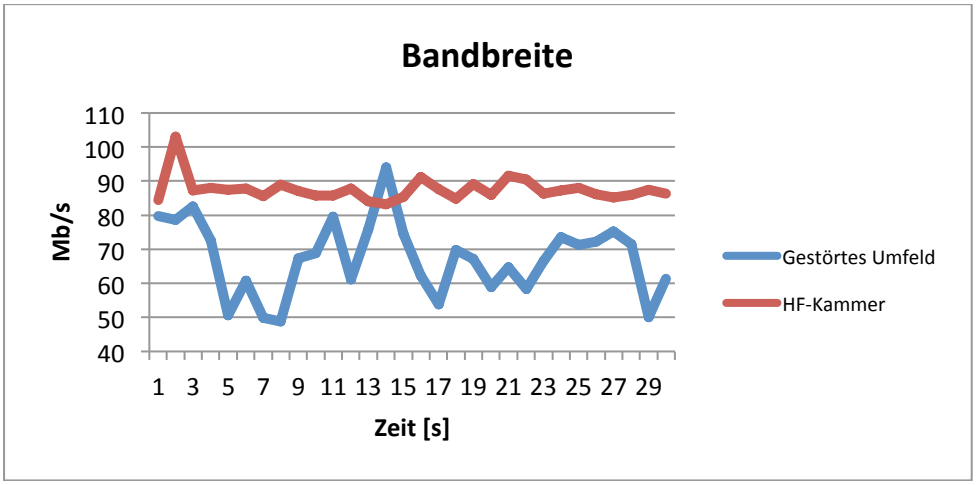
Durch die Analyse des Trace-Files wurde auch ersichtlich, dass bei der Aggregation der Frames der RTS/CTS-Mechanismus aktiviert wird. Das ist deshalb so, weil der RTS-Threshold bei den meisten Access Points auf 2347 Byte gesetzt ist. Da ein einzelnes 802.11-Frame maximal 2346 Byte lang sein darf, kommt deshalb der RTS/CTS-Mechanismus nicht zum Einsatz. Mit der Aggregation von Frames wird eine AMPDU bis zu 65’535 Byte lang. Daraus folgt, dass der RTS/CTS-Mechanismus wieder angewendet wird, sobald zwei oder mehr Frames aggregiert werden.

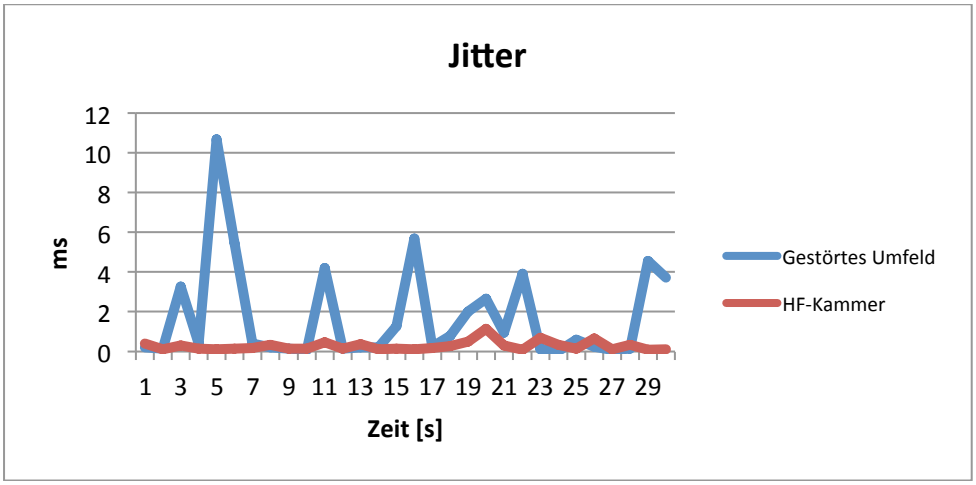
Im ungestörten Umfeld gab es zwischen den Messsekunden 21 und 22 einen Einbruch um fast 20 Mb/s. In dieser Zeit wurden sehr viele Frames vom Access Point nicht empfangen, sodass der Client diese Frames noch einmal senden musste, da er vom Access Point kein Block-ACK-Frame erhalten hatte. Zusätzlich ist auch erkennbar, dass in den ausgesendeten Block-ACK-Frames viele Frames

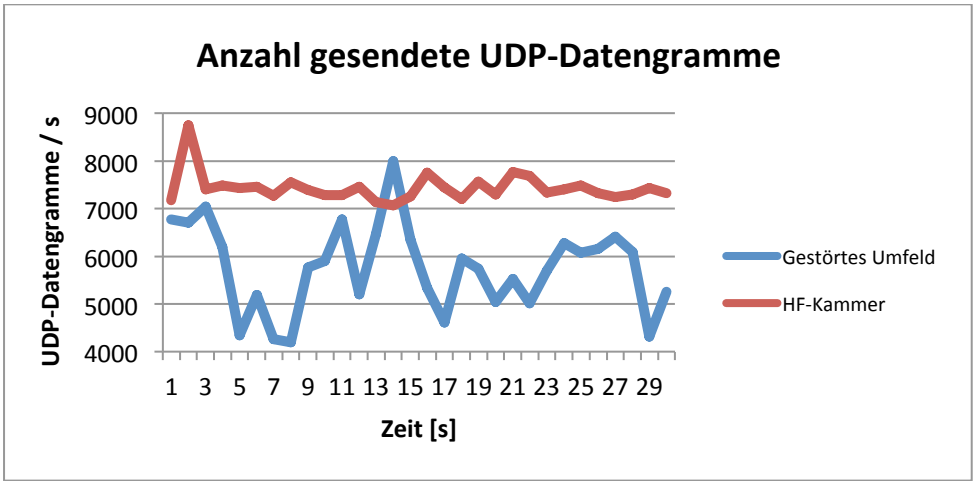
nicht bestätigt wurden, was bedeutet, dass der Access Point diese nicht empfangen hat. Wenn mehrmals hintereinander die Block-ACK-Frames eine gewisse Anzahl an nicht bestätigten Frames enthalten, dann wird der Block-ACK-Mechanismus für eine kurze Zeit deaktiviert und es wird auf das normale ACK-Verfahren umgeschaltet. All dies hat einen grossen Einfluss auf die Anzahl UDP-Datengramme pro Sekunde. Des Weiteren ist in dieser Zeit sichtbar, dass viele Frames aufgezeichnet wurden, welche nicht zu dieser Messung gehören. Das bedeutet, dass in dieser Zeit grosse Interferenzen aufgetreten sind. Dies ist auch daran erkennbar, dass viele RTS-Frames zwei- bis dreimal gesendet wurden und in dieser Zeit eine erhöhte Anzahl verlorener UDP-Datengramme verzeichnet wurde.

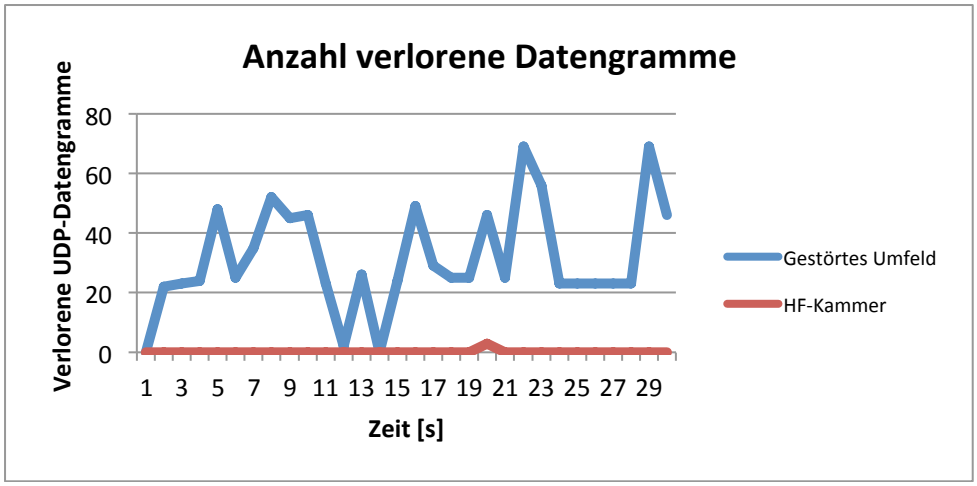
NETGEAR

Bei der Messung des Short-Guard-Intervalls wurde sowohl die Aggregation von Frames als auch die Verwendung von RIFS deaktiviert.









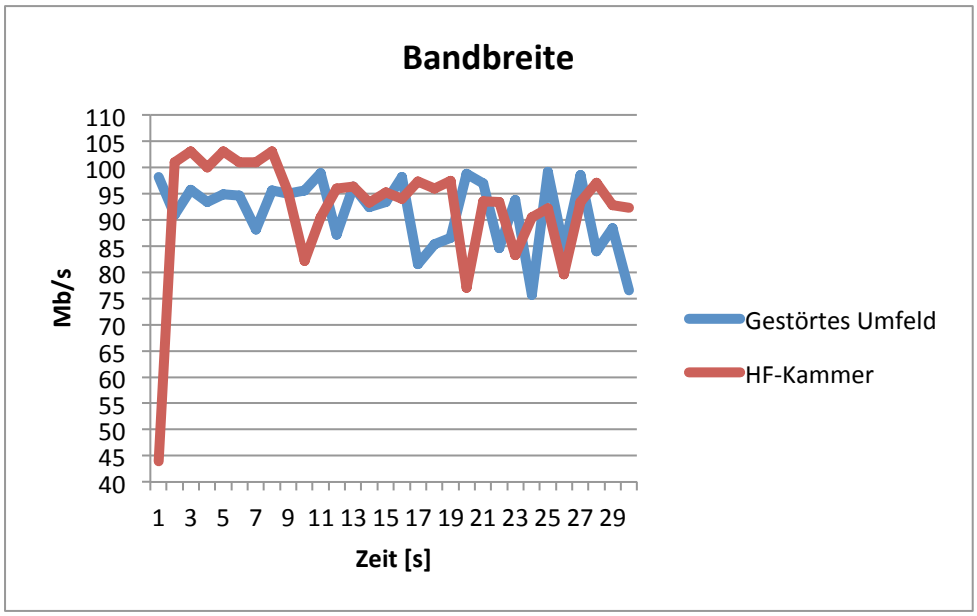
Bei diesen Messungen ist aufgefallen, dass trotz der Deaktivierung der Aggregation von Frames in beiden Messdurchführungen eine Aggregation stattfand.

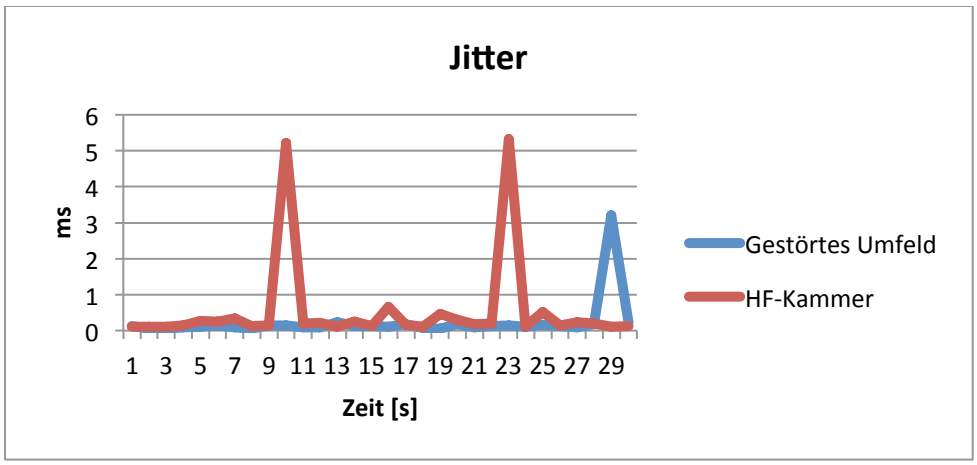
In der HF-Kammer ist klar erkennbar, dass die Anzahl gesendeter UDP-Datengramme in etwa konstant ist. Dementsprechend ist auch die Bandbreite konstant. Des Weiteren ist auch der Jitter sehr konstant. Wie zu erkennen ist, gab es in der HF-Kammer nur drei UDP-Datengramme, die nicht beim Empfänger ankamen.

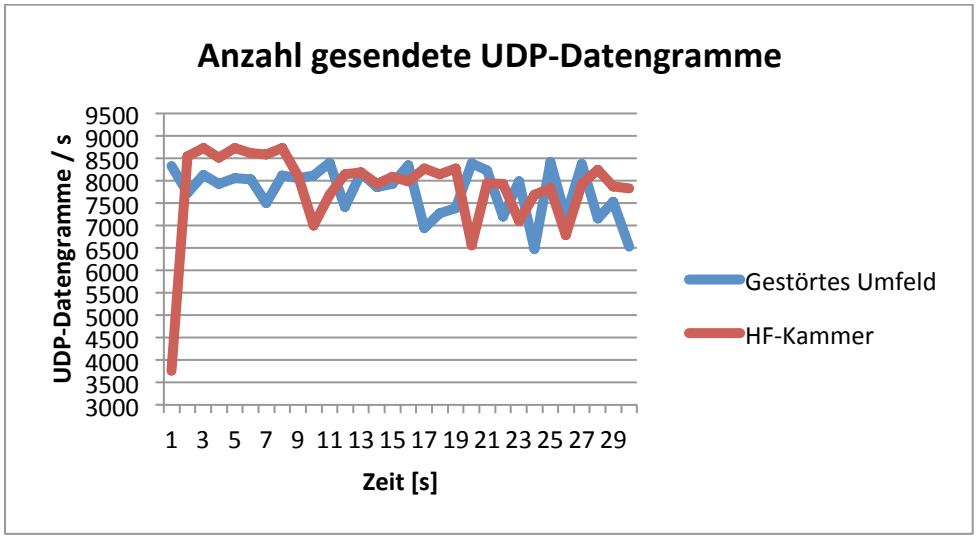
Im gestörten Umfeld ist die Anzahl gesendeter UDP-Datengramme pro Sekunde sehr variabel. Auffällig ist auch, dass der Jitter sehr stark schwankt. In den Zeiten, in denen hohe Jitter-Werte auftreten, ist sowohl in den Trace-Files als auch in der Anzahl gesendeter UDP-Datengramme erkennbar, dass weniger Frames vom Client zum Empfänger gesendet wurden. In den Trace-Files wurden auch viele 802.11-Frames aufgezeichnet, welche nicht zu der Messung gehören. Das bedeutet, dass viele Interferenzen von anderen WLANs auftraten. Dies zeigt sich auch in der Tatsache, dass sehr viele RTS-Frames doppelt und oder öfter übertragen werden mussten, bis der Client Zugriff auf das Medium erhielt und seine UDP-Datengramme senden durfte.

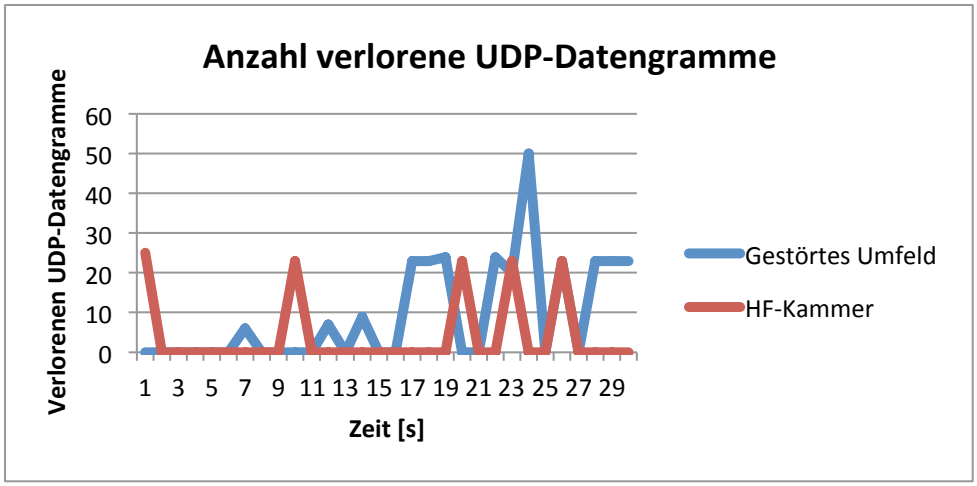
LONG GUARD, 20 MHZ KANALBREITE

CISCO







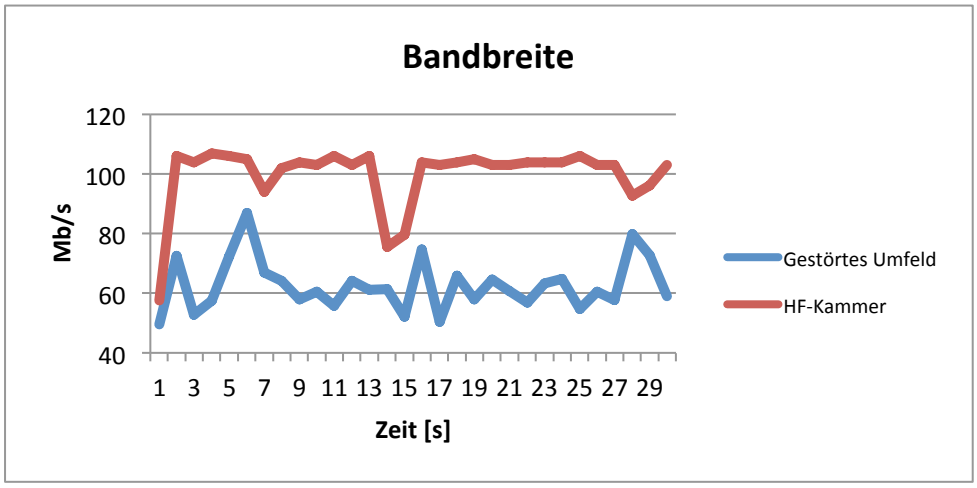


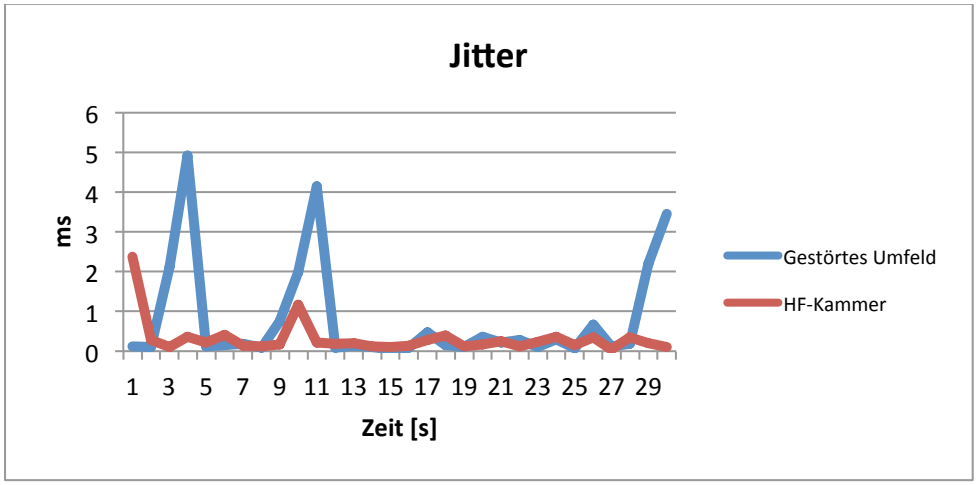
Der Vergleich zwischen Short Guard und Long Guard zeigt, dass durch die Verwendung des Long-Guard-Intervalls die Bandbreite reduziert wird. Der Grund für diesen Zusammenhang ist, dass beim Long Guard zwischen zwei ausgesendeten OFDM-Symbolen eine Pause von 800 ns eingelegt wird. Diese Wartezeit ist doppelt so lang wie beim Short Guard.

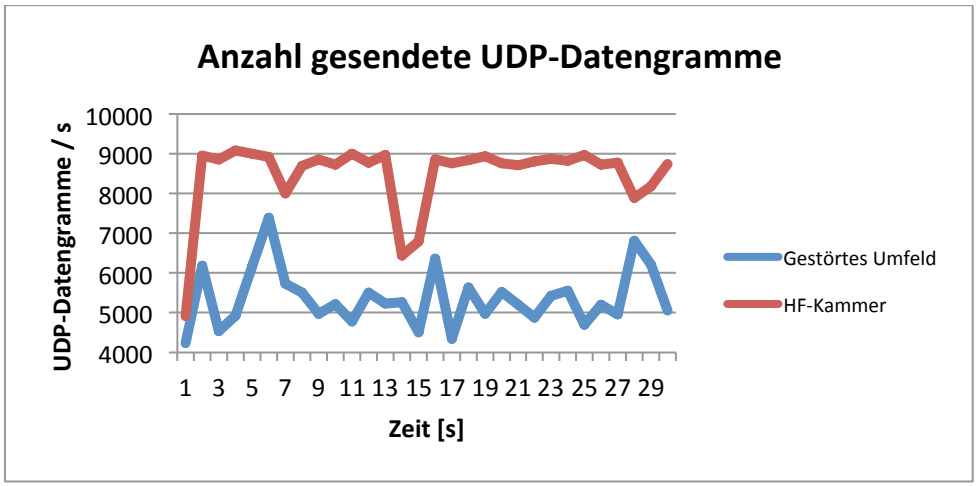
Im gestörten Umfeld ist wieder zu erkennen, dass starke Schwankungen bei der Bandbreite und der Anzahl gesendeter UDP-Datengramme auftreten. Bezüglich der Zeiten, in denen die Schwankungen auftreten, ist wieder zu erkennen, dass Block-ACK-Frames vom Access Point nicht ausgesendet wurden. Nachdem das Block-ACK-Frame nicht empfangen wurde, schaltet der Client wieder auf den normalen Block-ACK-Mechanismus um. Daher werden wieder alle Frames einzeln bestätigt. Interessant ist, dass, obwohl jedes Frame einzeln bestätigt wird, trotzdem der RTS/CTS-Mechanismus aktiv bleibt, obwohl die Frame-Länge unterhalb des RTS-Thresholds liegt. Dies hat einen enormen Einfluss auf die Anzahl übertragener Frames. Des Weiteren ist innerhalb dieser Schwankungen sichtbar, dass nicht alle einzelnen Frames bestätigt worden sind. Somit führen die nicht bestätigten Frames dazu, dass UDP-Datengramme verloren gehen. Dies zeigt sich auch in der Anzahl verlorener UDP-Datengramme.

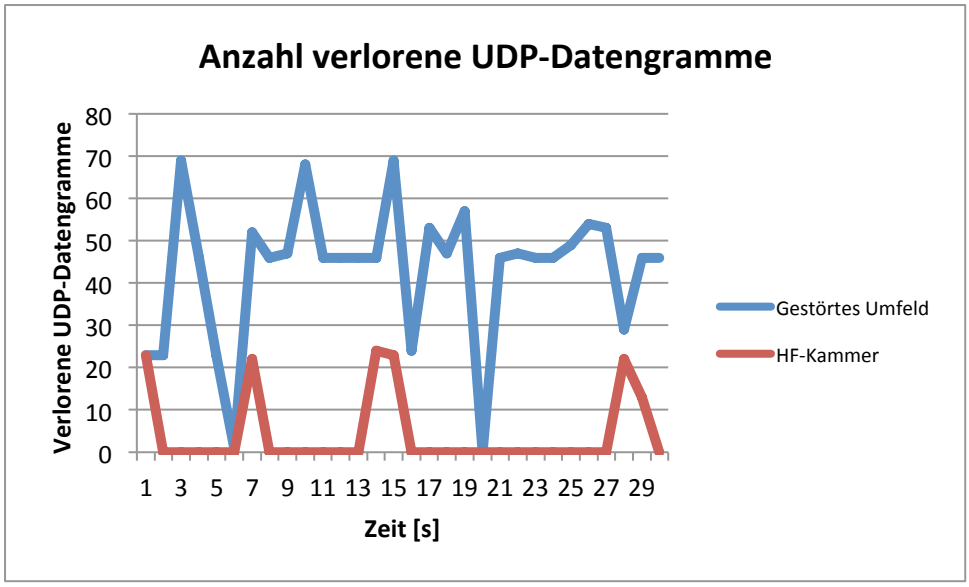
In der HF-Kammer ist am Anfang wieder der langsame Anstieg der Anzahl UDP-Datengramme pro Sekunde erkennbar. Dies liegt wiederum daran, dass während der ersten 200 ms kein Block-ACK-Mechanismus verwendet worden ist. Des Weiteren gibt es bei Sekunde 10, 20 und 26 starke Einbrüche. Hier wurden wieder Block-ACK-Frames nicht ausgesendet und es wurde wiederum auf den normalen Block-ACK-Mechanismus umgeschaltet.

NETGEAR


Bandbreite
Mb/s
120
100
80
60
40
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

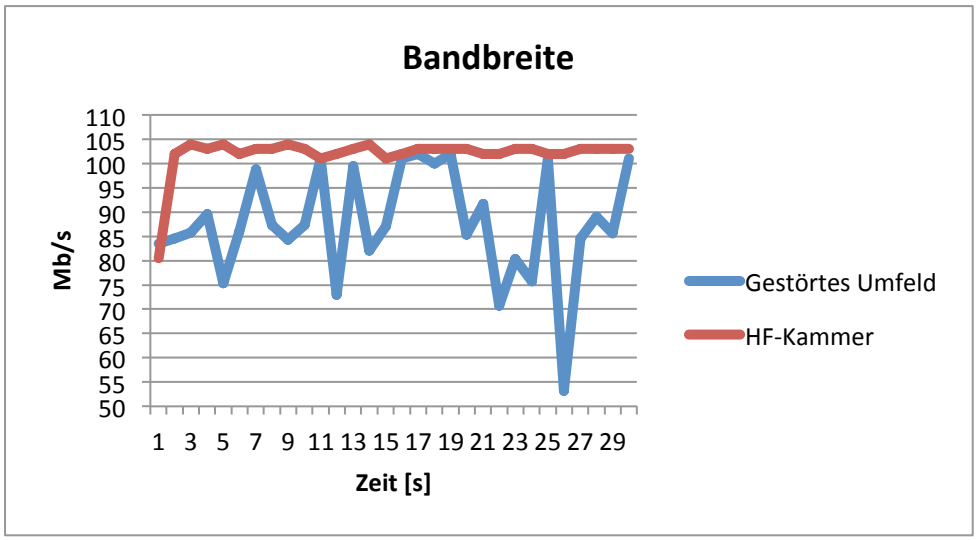

Jitter
ms
6
5
4
3
2
1
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

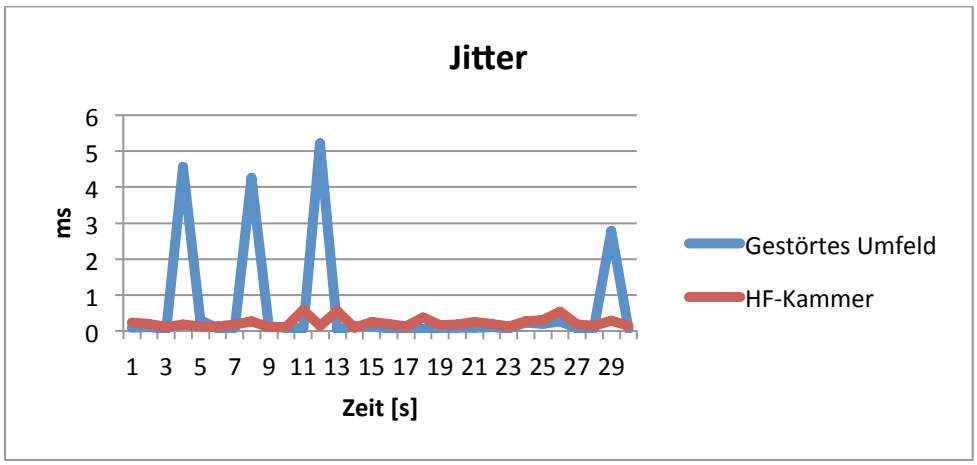

Anzahl gesendete UDP-Datengramme
UDP-Datengramme / s
10000
9000
8000
7000
6000
5000
4000
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

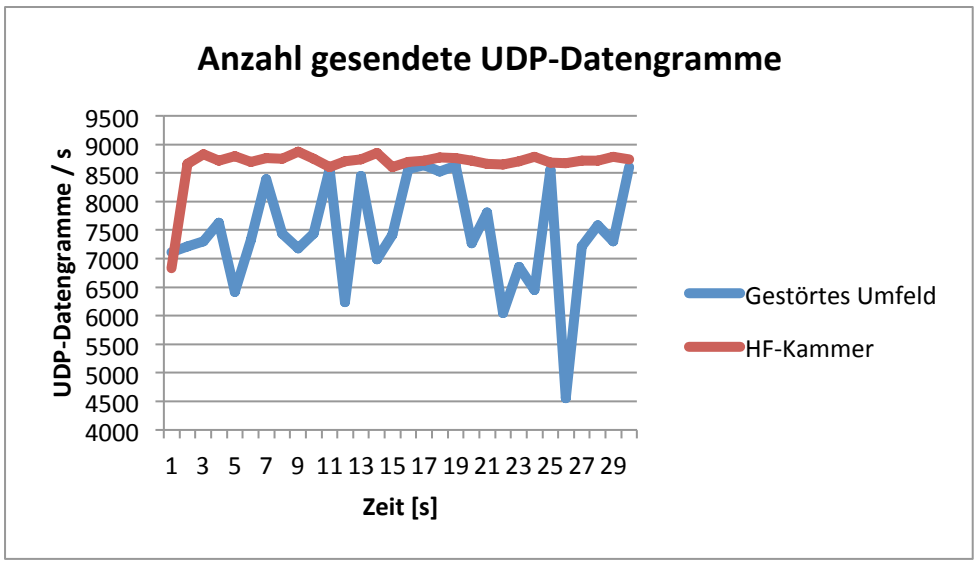

Anzahl verlorene UDP-Datengramme
Verlorene UDP-Datengramme
80
70
60
50
40
30
20
10
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

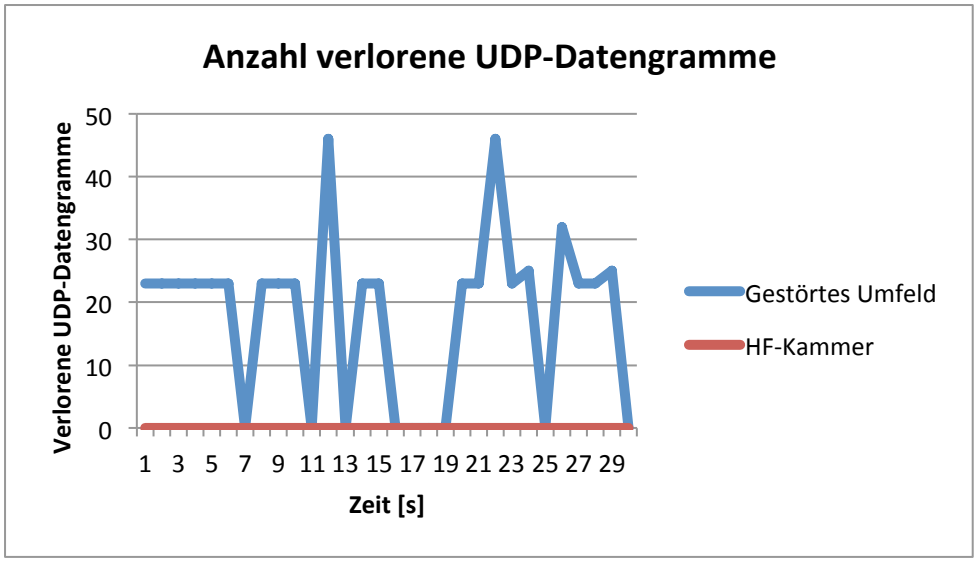
SHORT GUARD, 40 MHZ KANALBREITE

CISCO







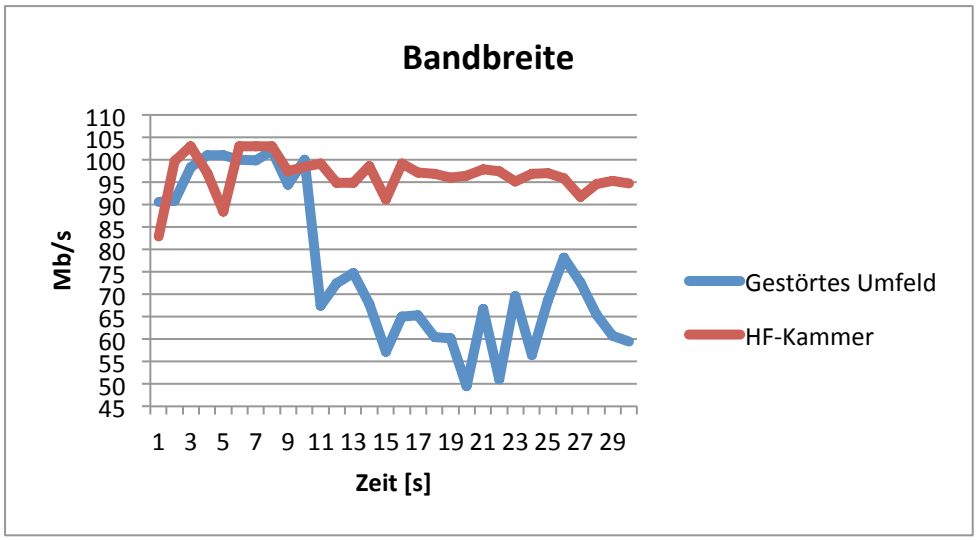


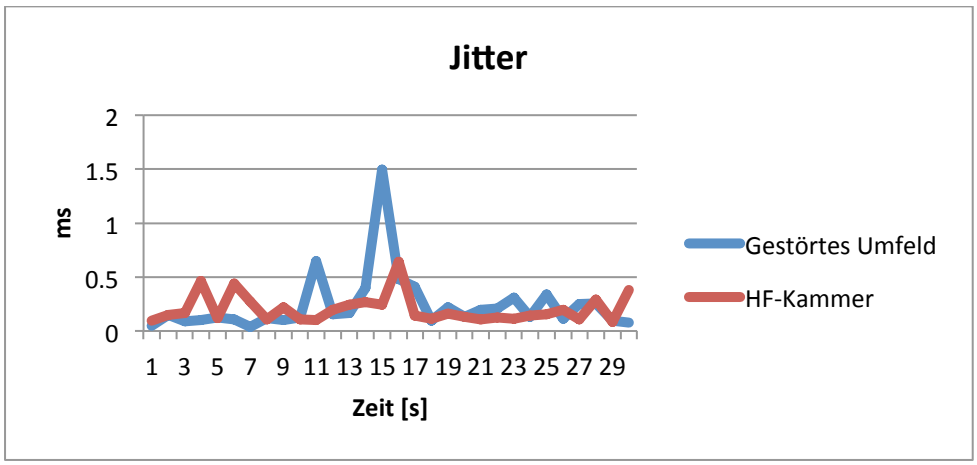
Die Messung des Short-Guard-Intervalls im 40-MHz-Kanal zeigt deutlich, welch grossen Einfluss Interferenzen auf den Durchsatz im WLAN haben. Der Cisco Access Point unterstützt nur das 2.4-GHz-Frequenzband. Durch die Aggregation von zwei benachbarten Kanälen wird fast das ganze Frequenzband benutzt. Dadurch erhöht sich auch der Störeinfluss auf das WLAN enorm, weil mehrere andere WLANs und andere Störquellen auf diesen Frequenzbereichen vorhanden sind.

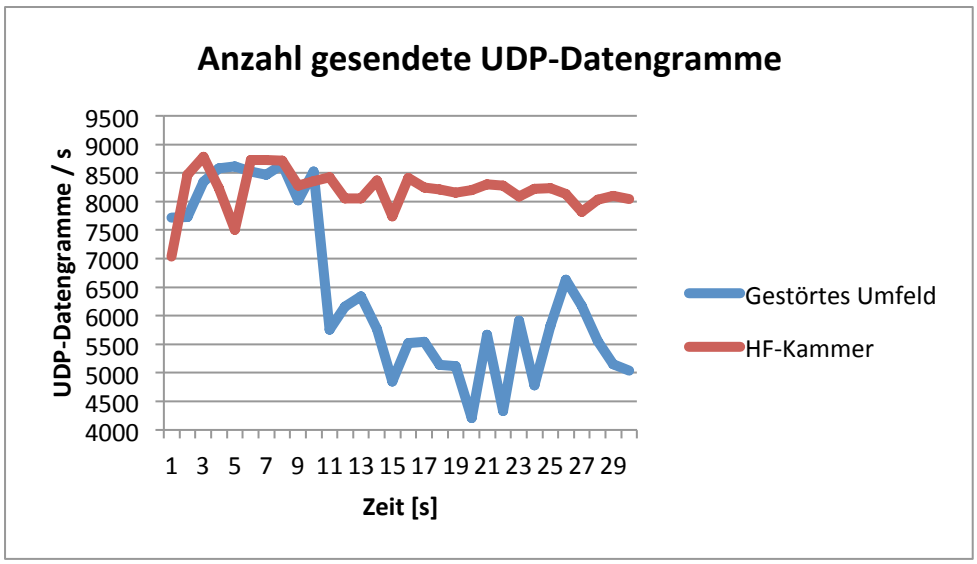
Vergleicht man die Messungen in der HF-Kammer mit denen in der gestörten Umgebung, so ist eindeutig zu erkennen, dass Interferenzen einen enormen Einfluss auf WLANs haben. In der HF-Kammer ist die Anzahl UDP-Datengramme pro Sekunde praktisch konstant. Daraus resultiert auch eine konstante Bitrate. Bei der Messung in der gestörten Umgebung ist ersichtlich, dass bei den tiefen Werten wieder auf den normalen ACK-Mechanismus umgeschaltet wurde. Dabei wurden wieder sehr oft ACK- und RTS-Frames doppelt oder öfter ausgesendet, was darauf hindeutet, dass diese nicht auf Anhieb beim Empfänger ankamen. Dies weist darauf hin, dass als Folge der Interfenzen diese Frames bei der Übertragung über die Luft verloren gingen.

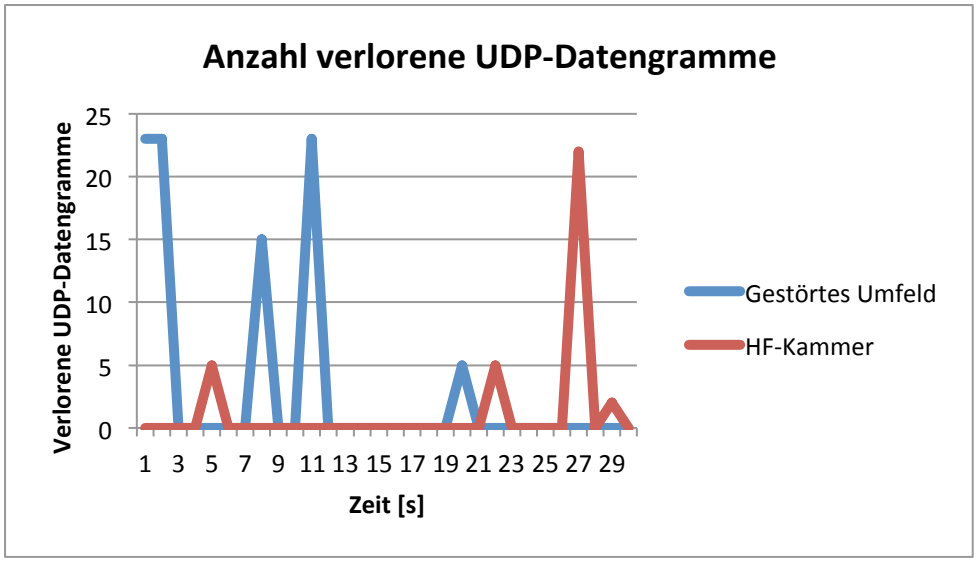
LONG GUARD, 40 MHZ KANALBREITE

CISCO







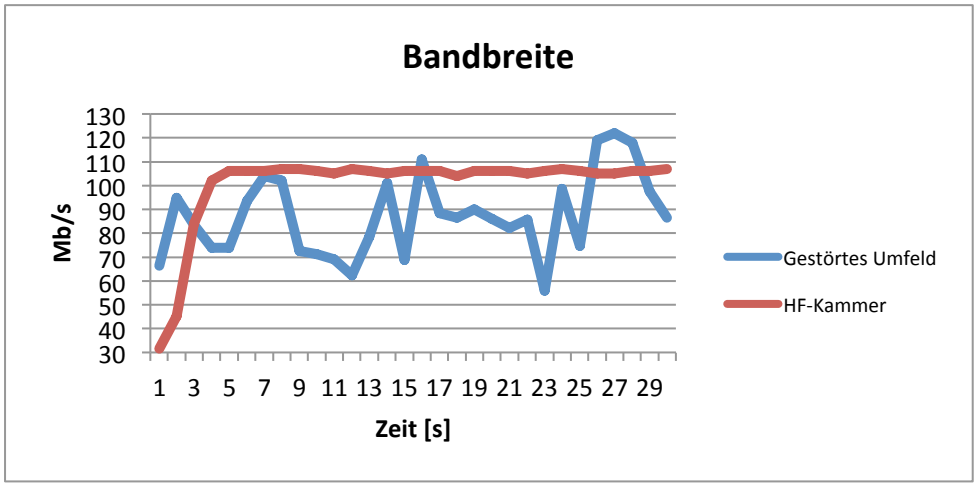


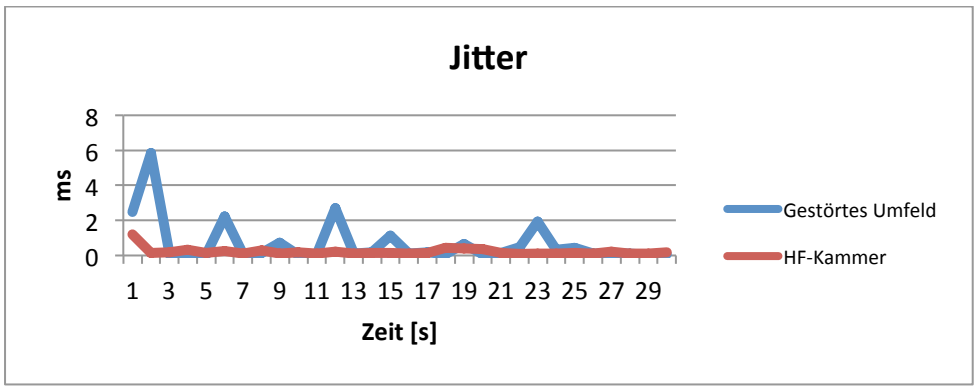
Auch in dieser Messung ist erkennbar, dass Interferenzen den Durchsatz enorm einschränken. Im gestörten Umfeld ist zu erkennen, dass die Bandbreite im Vergleich zur Verwendung des Short-Guard-Intervalls noch tiefere Werte erreicht hat. Ein Grund dafür ist, dass mit dem Long-Guard-Intervall die Frames länger über das Medium übertragen werden als beim Short Guard, weil die Pause zwischen zwei ausgesendeten Symbolen nun 800 ns dauert. Somit dauert das Aussenden eines Frames länger als mit dem Short-Guard-Intervall. Dies führt dazu, dass ein ausgesendetes Frame länger gestört werden kann als eines, das mit dem Short Guard übertragen wird. Es erklärt auch, warum im 40-MHz-Bereich und unter Verwendung des Long-Guard-Intervalls viel weniger UDP-Datengramme pro Sekunde übertragen werden können, da viele ausgesendete Frames gestört wurden und deshalb nicht empfangen werden konnten.

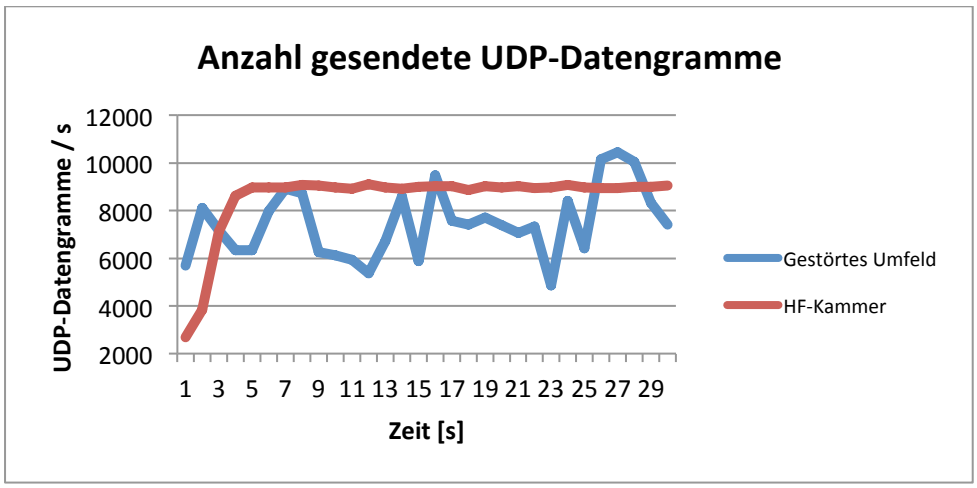
FRAME-AGGREGATION

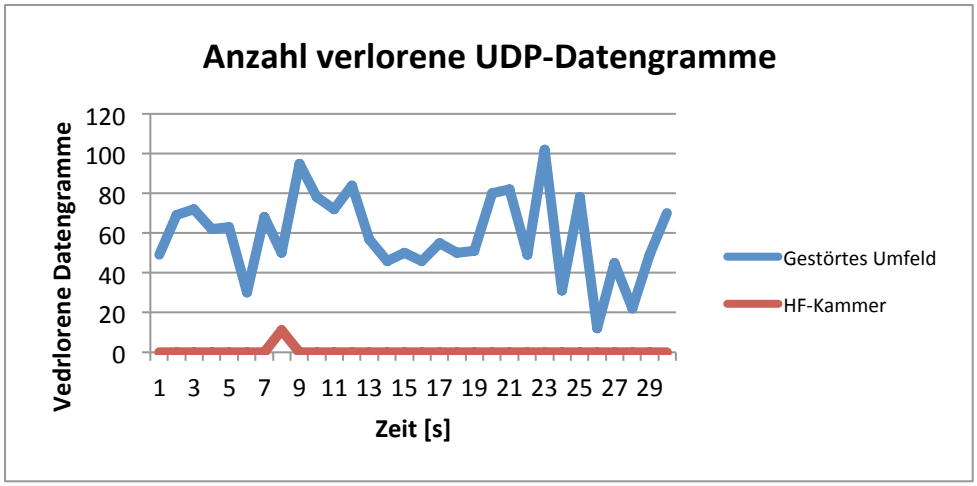
Wie bei Cisco wird bei der Aggregation von Frames der RTS/CTS-Mechanismus aktiviert, da der RTS-Threshold von 2347 Byte durch die Aggregation überschritten wird.

NETGEAR 20 MHZ KANALBREITE









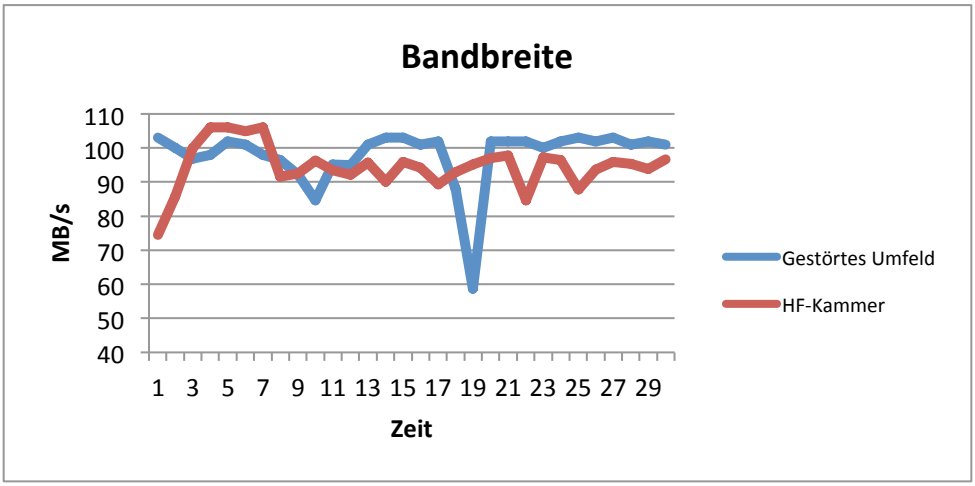
Hier ist auch wieder auffällig, dass zu Beginn keine Aggregation von Frames stattfand. Das heisst, dass am Anfang der normale ACK-Mechanismus benutzt wurde.

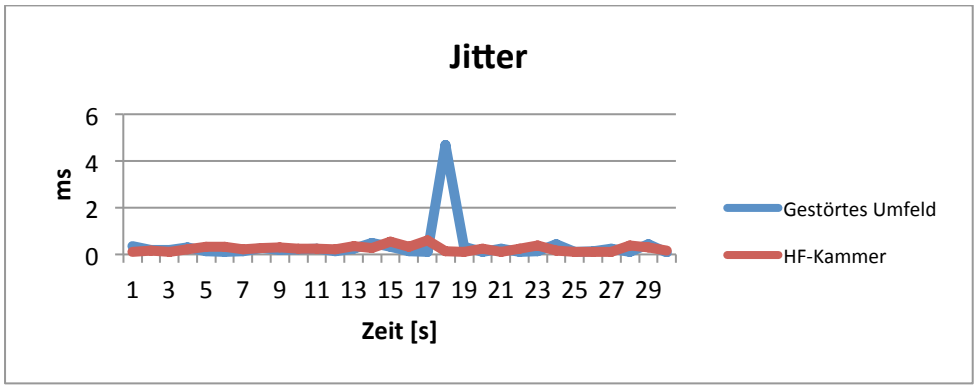
In der HF-Kammer wurde der Block-ACK-Mechanismus nach zwei Sekunden aktiviert, was sich auch in der Anzahl ausgesendete UDP-Datengramme widerspiegelt. Dadurch ging auch die Bandbreite nach oben.

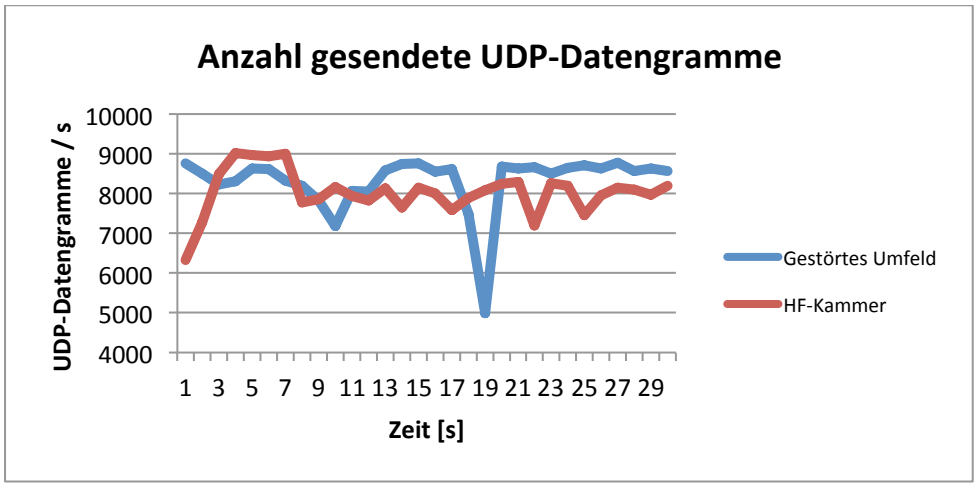
Die Messung im gestörten Umfeld zeigt wieder deutliche Schwankungen in der Anzahl gesendeter UDP-Datengramme. Dabei wird in den Trace-Files wieder deutlich, dass viele 802.11-Frames aufgezeichnet worden sind, die nicht zur Messung gehören. Das ist wieder das Resultat von Interferenzen anderer WLANs. Dabei ist erkennbar, dass in dieser Zeit kaum Frames aggregiert wurden. Das zeigt sich dann auch wieder in der Anzahl gesendeter UDP-Datengramme, welche dadurch stark verringert wurde.

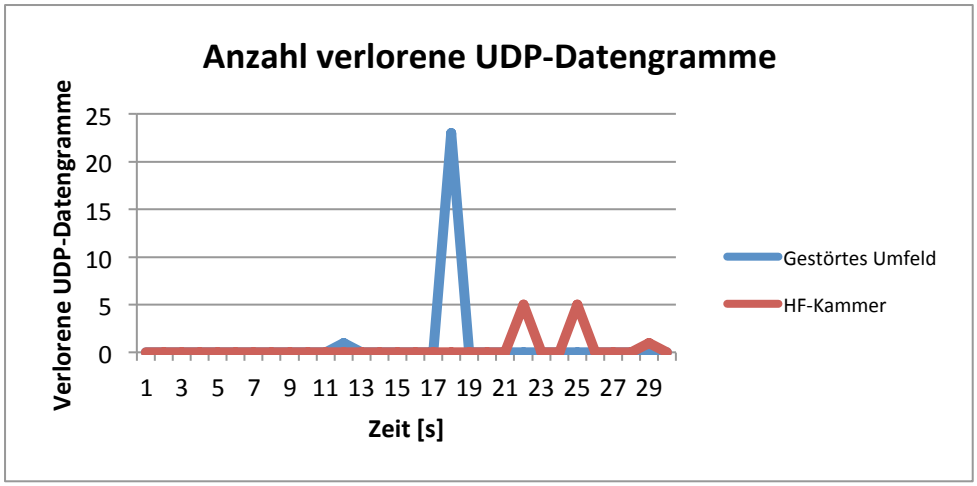
RIFS

NETGEAR, 20 MHZ KANALBREITE









Die Messungen mit RIFS zeigen, dass es nicht immer sinnvoll ist, Frames zu aggregieren. Die Aggregation von Frames macht hauptsächlich bei Burst-artigem Verkehr Sinn. Bei den Messungen mittels UDP wird allerdings mit einer konstanten Datenrate gesendet, sodass ein konstanter Verkehr vorhanden ist. Vergleicht man die Messungen mit RIFS mit denen unter Frame-Aggregation, so ist erkennbar, dass über die Zeit mehr Frames gesendet werden konnten, als es mit Aggregation der Fall ist. Bei der Aggregation von Frames wird auf eine gewisse Anzahl bzw. Gesamtlänge an Frames gewartet, bis diese dann gesendet werden. Somit kann es zu Verzögerungen beim Aussenden von aggregierten Frames kommen. RIFS vermeidet die Verzögerung beim Aussenden, sodass jedes Frame einzeln ausgesendet wird, sobald der Zugriff auf das Medium erteilt wurde.

In der HF-Kammer stimmt die obige Aussage nicht hundertprozentig. Der Grund dafür ist, dass in der HF-Kammer keine Interferenzen vorhanden sind und die Station dadurch immer Zugriff auf das Medium erhält. Wenn die Station immer Zugriff auf das Medium hat, ist die Aggregation von Frames sehr effizient.

Im gestörten Umfeld ist dagegen zu erkennen, dass über die Gesamtzeit der Messung ca. 20'000 UDP-Datengramme mehr gesendet wurden, als es im selben Umfeld mit Aggregation von Frames der Fall war. Die durchschnittliche Bandbreite ist mit der Verwendung von RIFS um 10 Mbps höher. Daher ist im gestörten Umfeld ersichtlich, dass es aufgrund der Aggregation von Frames zu Verzögerungen kam. Dies ist deshalb so, weil das Medium nicht immer frei war und das Aussenden der aggregierten Frames deshalb verzögert wurde, was sich wiederum auf die Gesamtzahl der gesendeten UDP-Datengramme auswirkt. In der Messsekunde 19 wurde wieder erkannt, dass viele Frames aufgezeichnet wurden, welche nicht zur Messung gehören. Das ist wieder die Folge von Interferenzen. Durch diese konnte der Client weniger oft auf das Medium zugreifen und Daten senden.

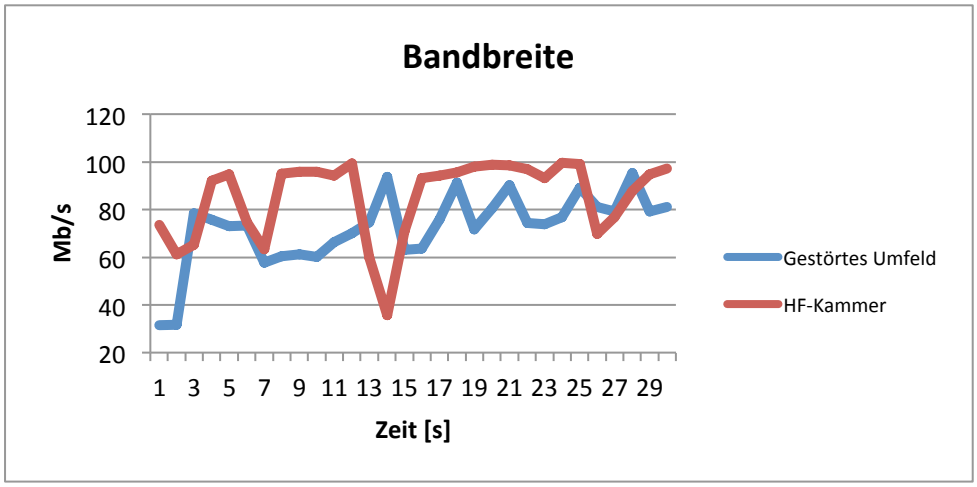
5-GHZ-FREQUENZBAND

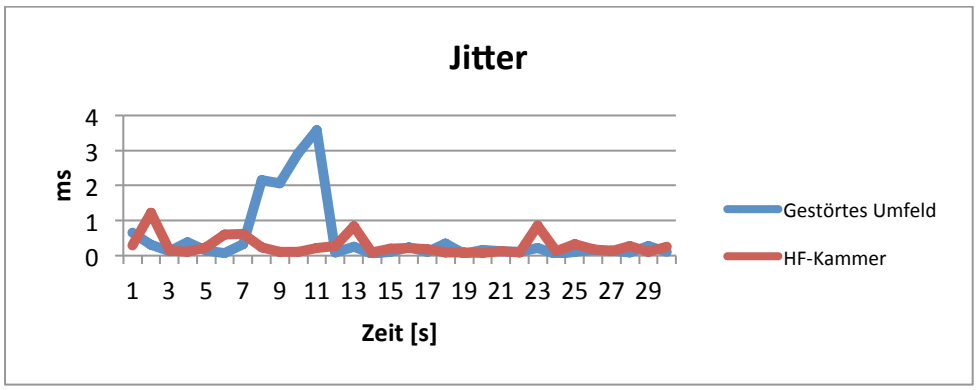
Im 5-GHz-Frequenzband wurden die Messungen nur mit dem Netgear Access Point ausgeführt, weil der Cisco Access Point das 5-GHz-Frequenzband nicht unterstützt.

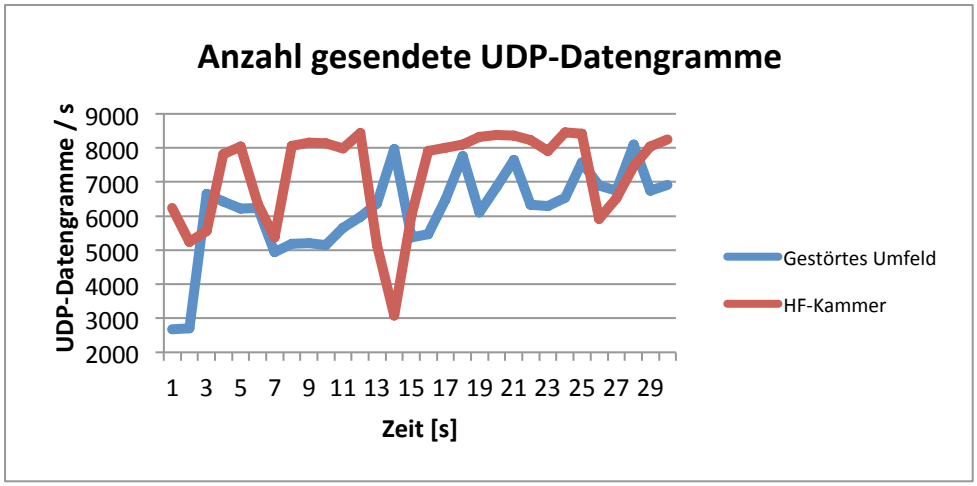
Im 5-GHz-Bereich ist bei einigen Messauswertungen wiederum auffallend, dass in der HF-Kammer schlechtere Werte erreicht wurden als im gestörten Umfeld. Dies liegt auch hier an der Verwendung der MIMO-Technologie, die im N-Standard eingesetzt wird. Erkennbar ist auch, dass im 5-GHz-Bereich ein grösserer Einfluss ersichtlich ist, als es im 2.4-GHz-Band der Fall war. Die Frage nach den Gründen hierfür konnte auch ein HF-Techniker nicht beantworten.

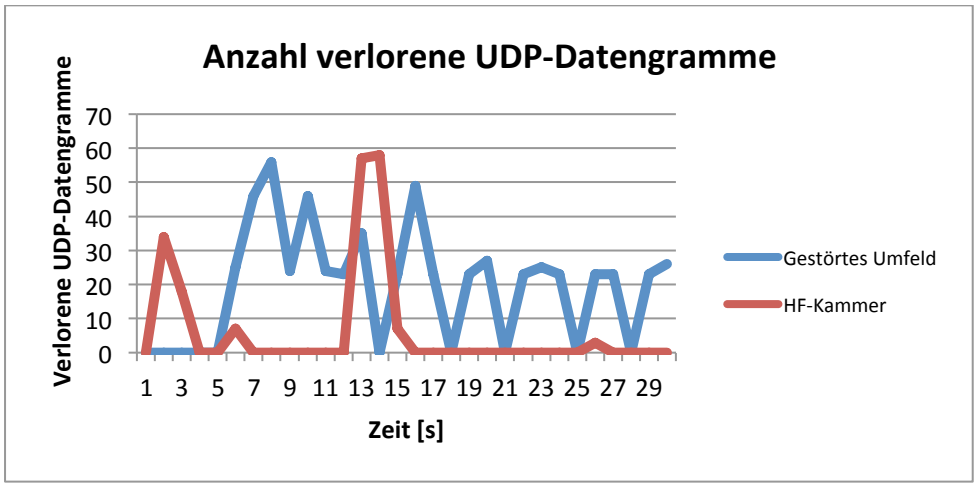
SHORT GUARD

20 MHZ KANALBREITE



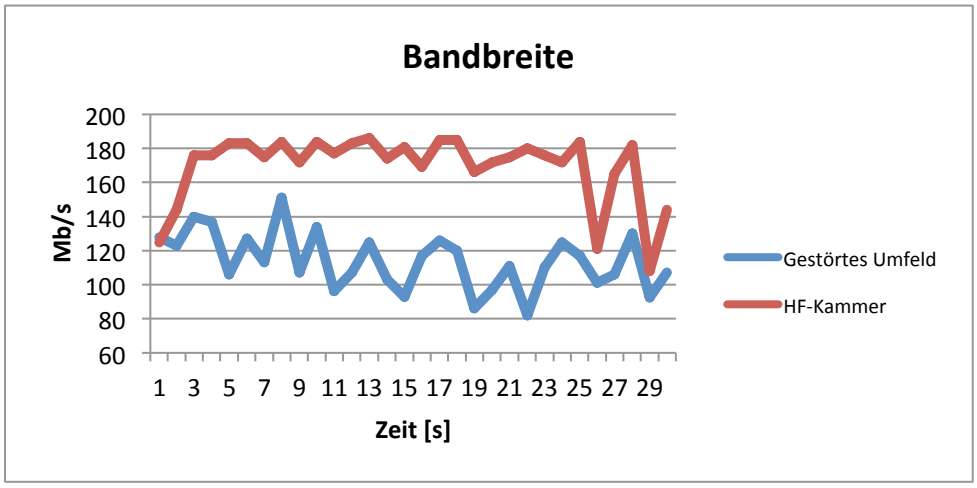


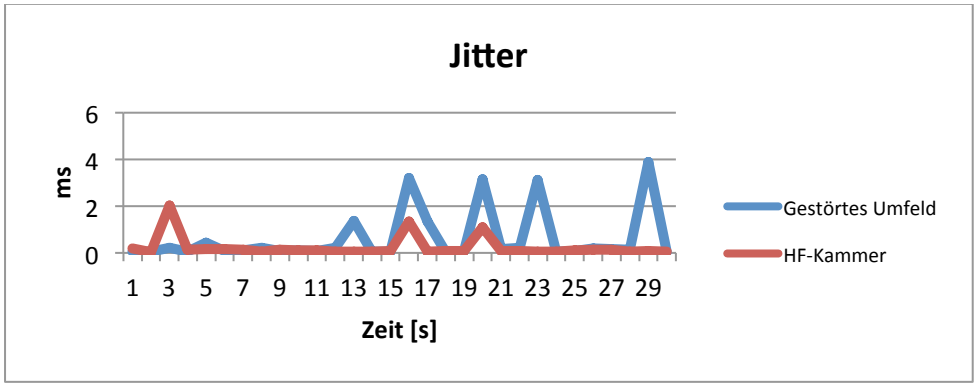


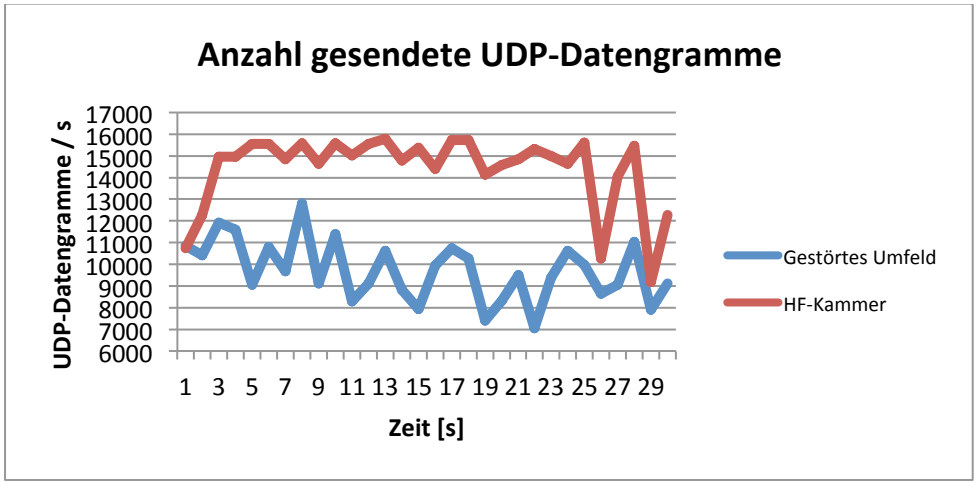


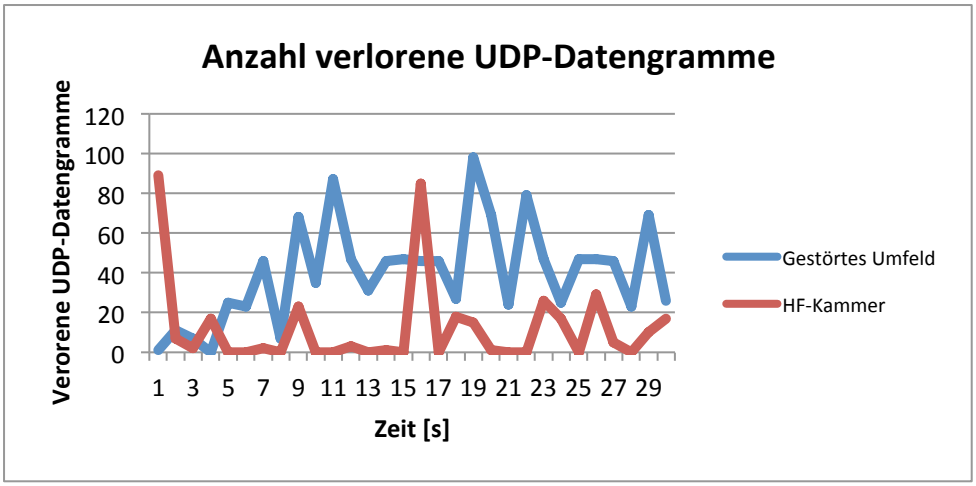
Bei der Verwendung des Short-Guard-Intervalls ist erkennbar, dass über die Gesamtzeit in der HF-Kammer mehr UDP-Datengramme ausgesendet werden konnten, als es im gestörten Umfeld der Fall war. In der HF-Kammer wurden 33'200 UDP-Datengramme mehr ausgesendet als im gestörten Umfeld. In der HF-Kammer gab es ein Tief in der Messsekunde 14. In dieser Sekunde war auch die Anzahl verlorener UDP-Datengramme relativ hoch, sie betrug zwei Prozent der Anzahl gesendeter UDP-Datengramme.

40 MHZ KANALBREITE





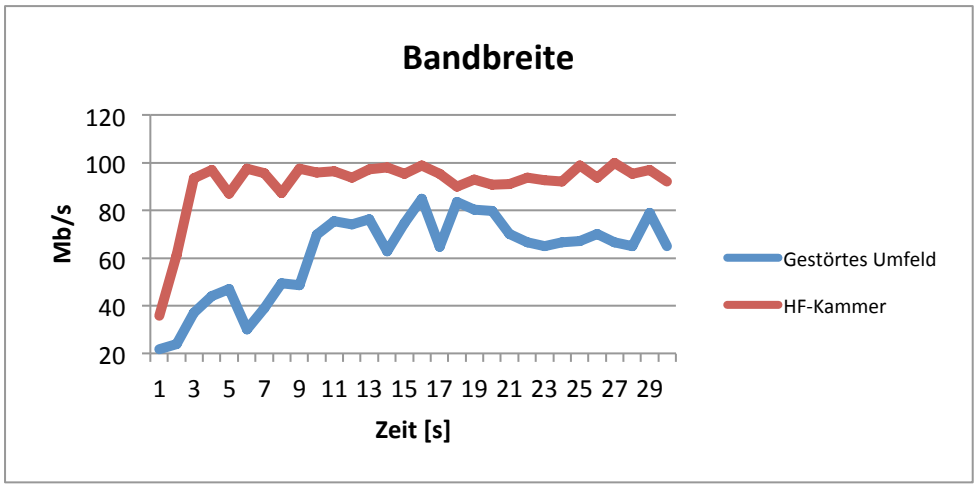


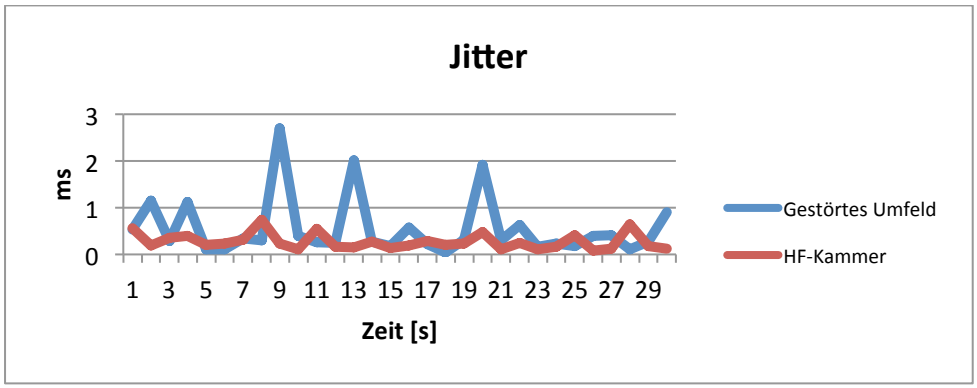


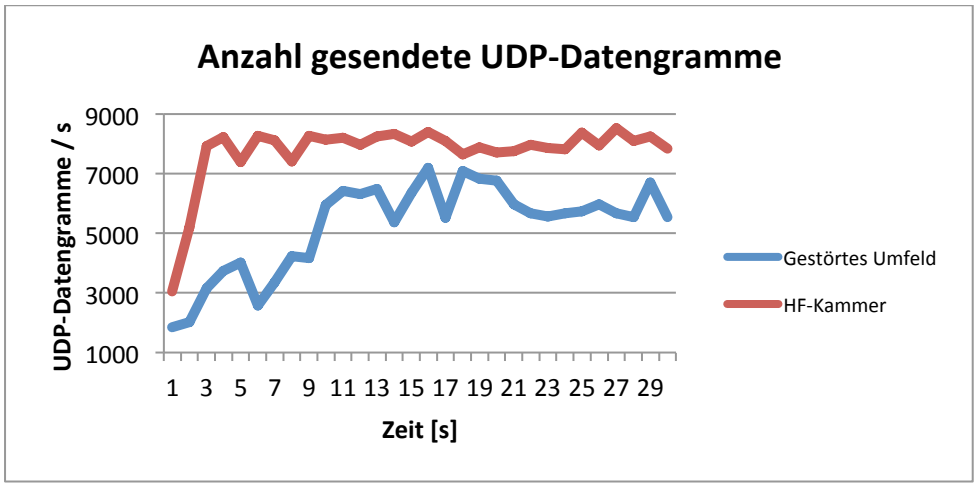
Bei der Verwendung einer Kanalbreite von 40 MHz in der HF-Kammer zeigt sich fast eine Verdoppelung der Anzahl gesendeter UDP-Datengramme im Vergleich zu einer Kanalbreite von 20 MHz. In den Messsekunden 26 und 29 fällt auf, dass die Anzahl gesendeter UDP-Datengramme stark zurückgegangen ist. Bei der Analyse der Trace-Files wurde deutlich, dass viele Segmente einer AMPDU vom Access Point nicht empfangen wurden und deshalb vom Client noch einmal ausgesendet werden mussten. Dies führte beim Client zu weiteren Verarbeitungszeiten, daher konnten weniger UDP-Datengramme ausgesendet werden.

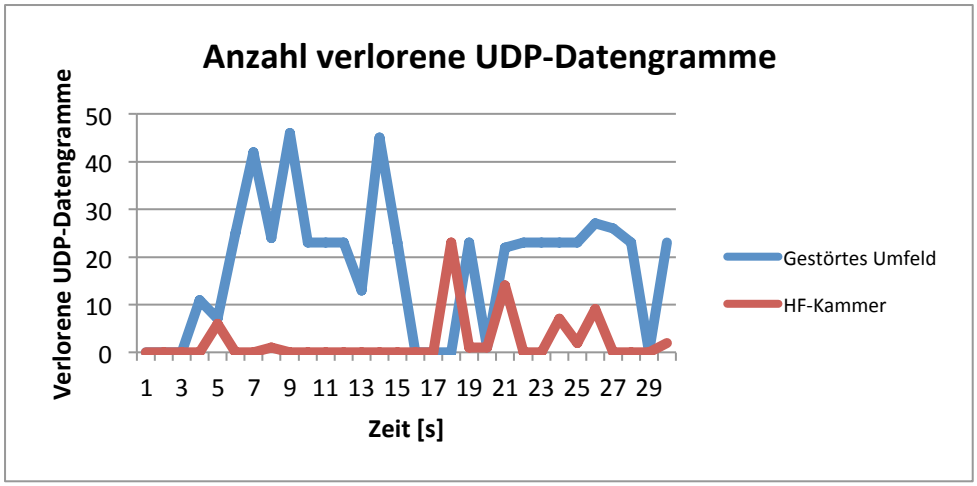
LONG GUARD

20 MHZ KANALBREITE

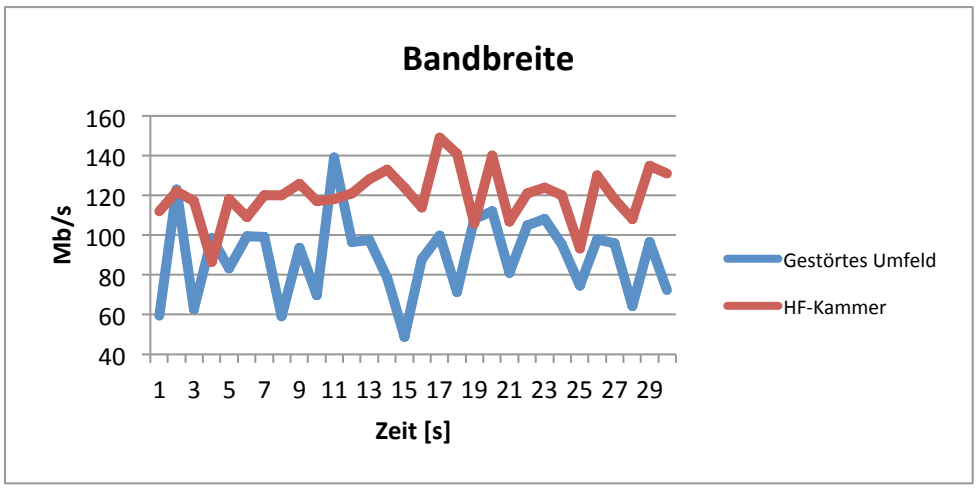


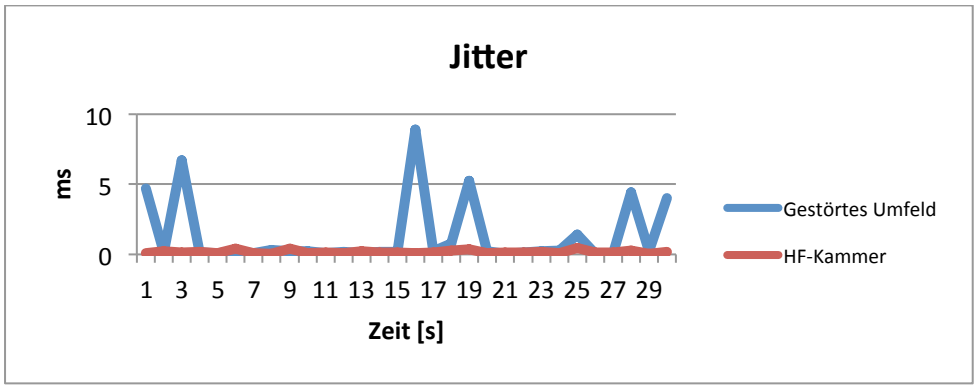


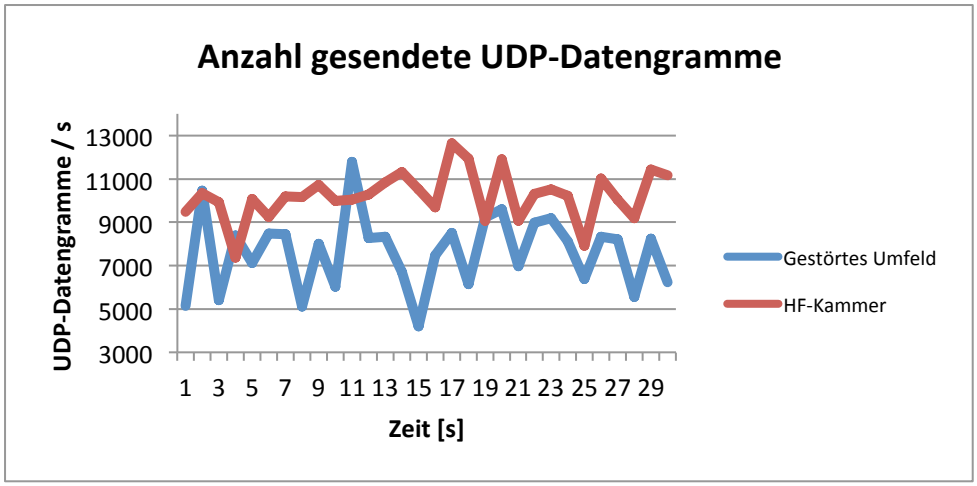


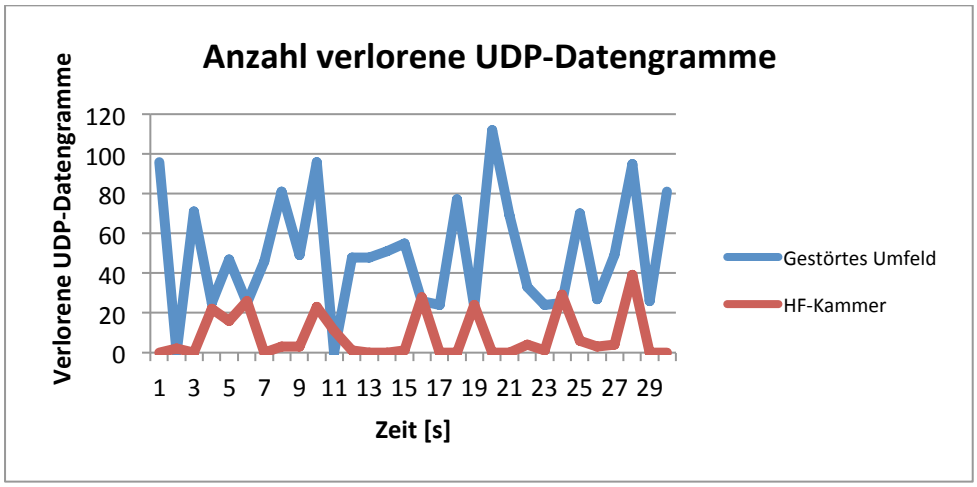


40 MHZ KANALBREITE





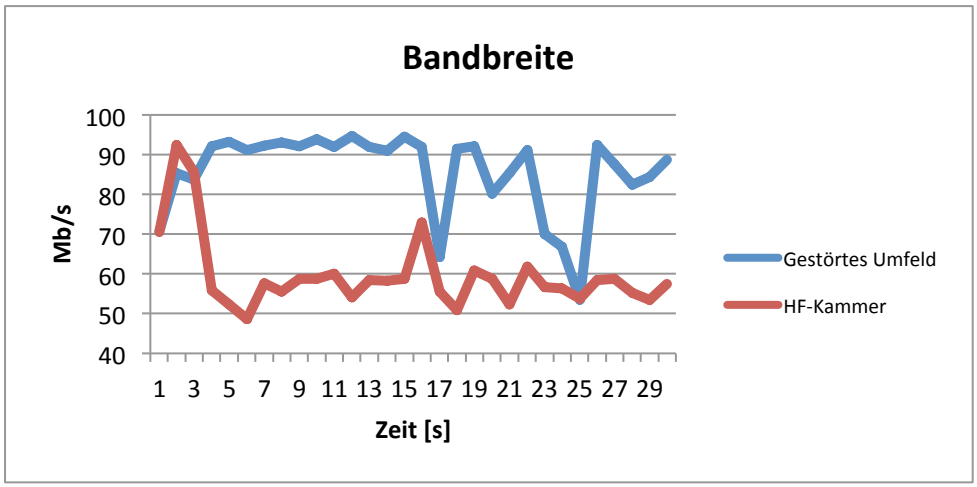


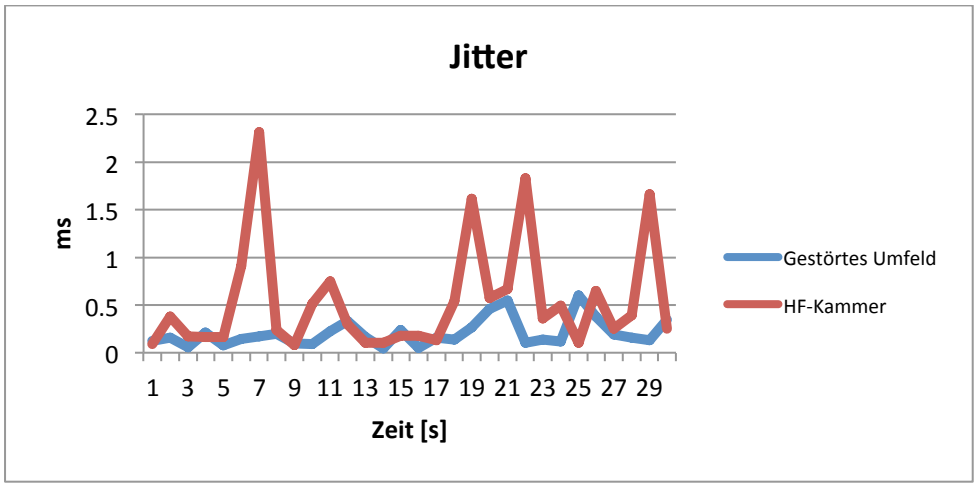


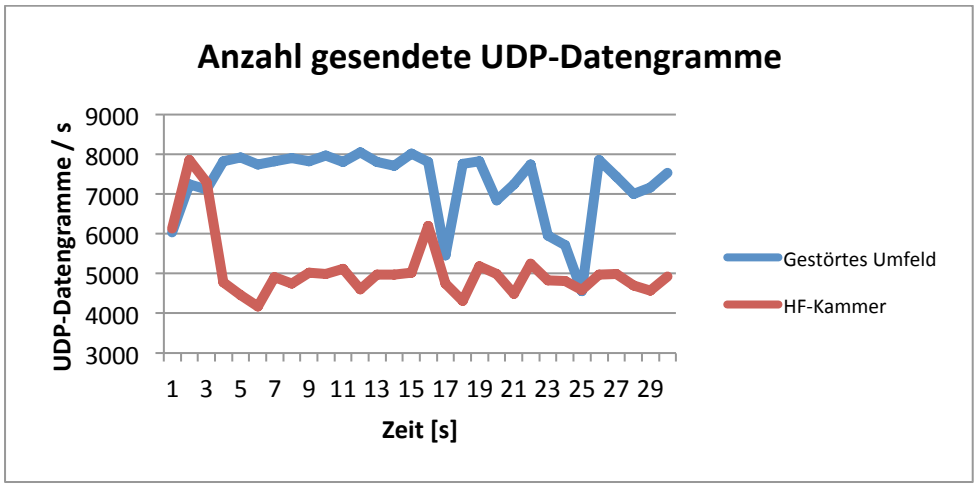
Vergleicht man die Messungen mit Long-Guard-Intervall mit derjenigen mit Short-Guard Intervall, so zeigt sich, dass das Short Guard einen grossen Einfluss auf den Durchsatz von WLANs hat. Beim Long-Guard- ist die Pause zwischen zwei OFDM-Symbolen doppelt so lang wie beim Short-Guard-Intervall. Dies hat natürlich auch einen Einfluss auf die Bandbreite. In der HF-Kammer konnten durch die Verwendung des Short-Guard-Intervalls 125'818 UDP-Datengramme mehr ausgesendet werden als mit dem Long-Guard-Intervall. Im gestörten Umfeld beträgt die Differenz 62'406 UDP-Datengramme.

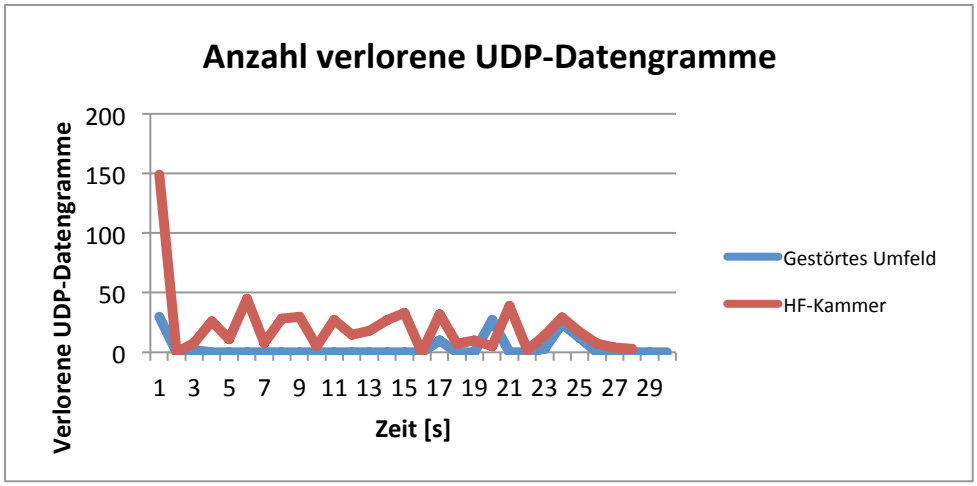
FRAME-AGGREGATION

20 MHZ KANALBREITE

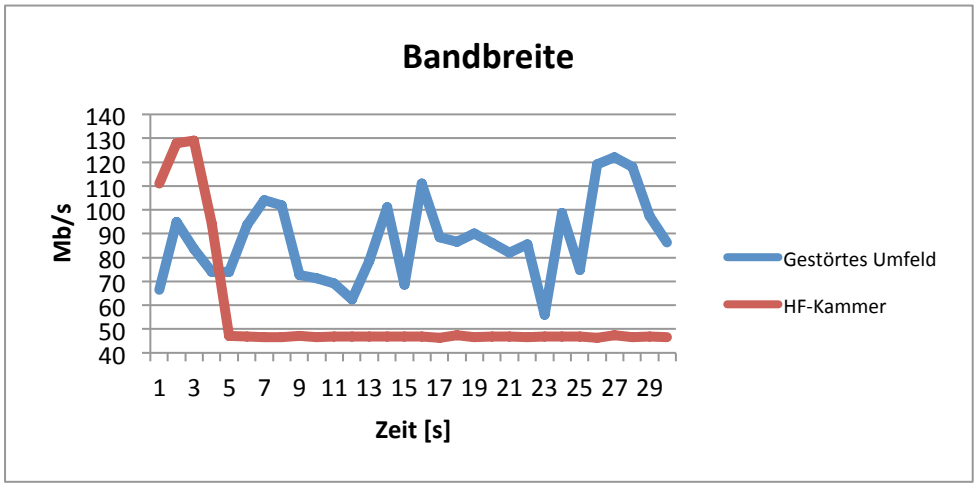


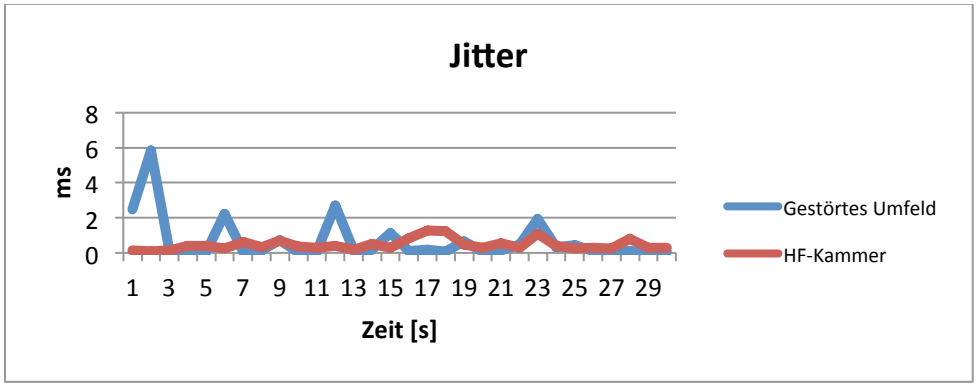


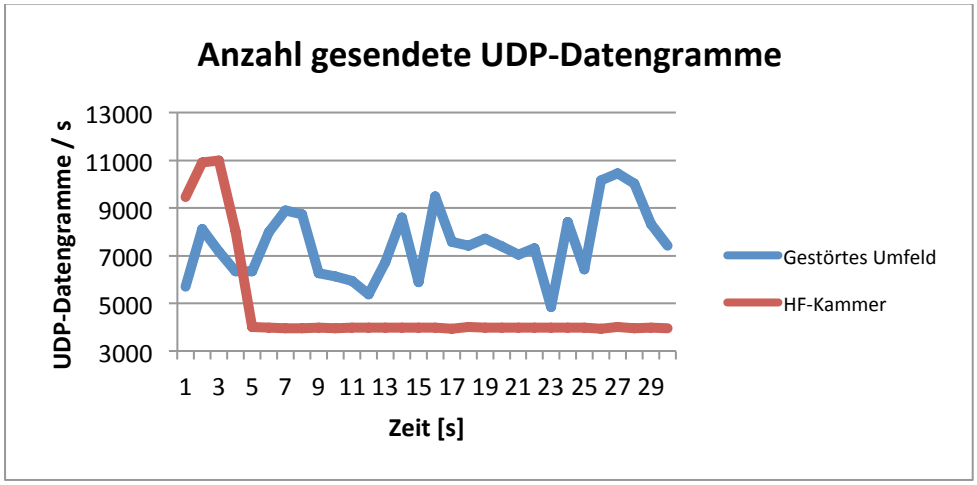


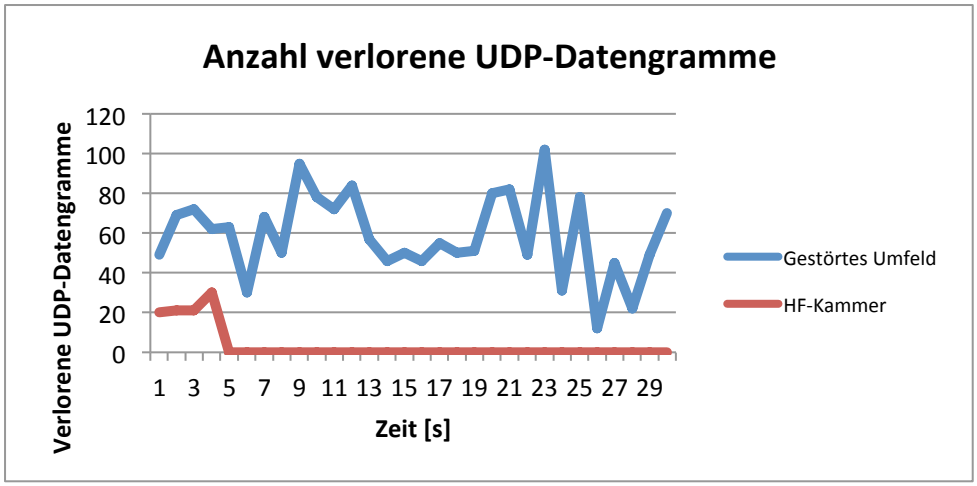

Anzahl verlorene UDP-Datengramme
Verlorene UDP-Datengramme
200
150
100
50
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

40 MHZ KANALBREITE



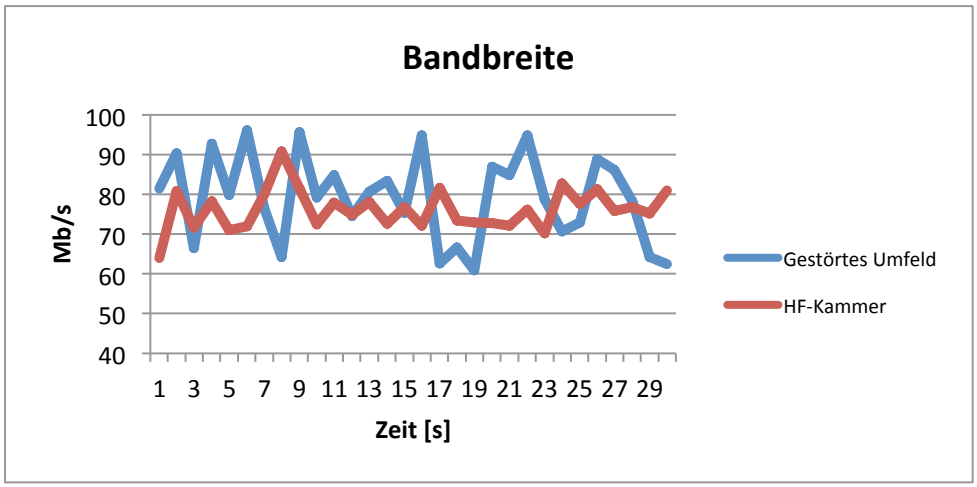


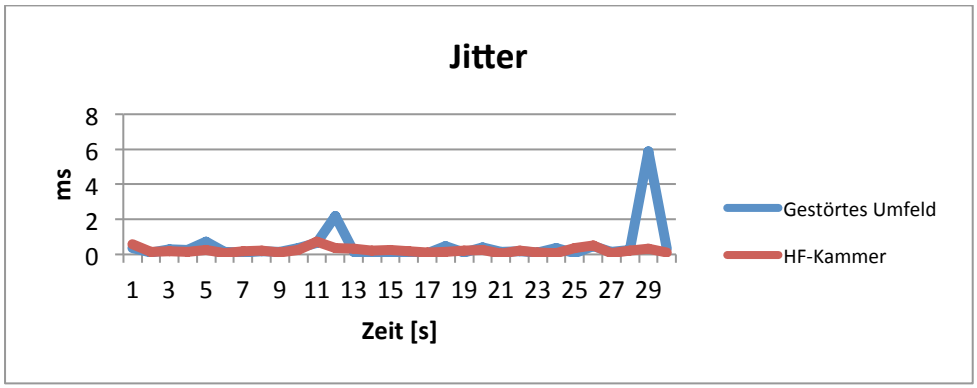


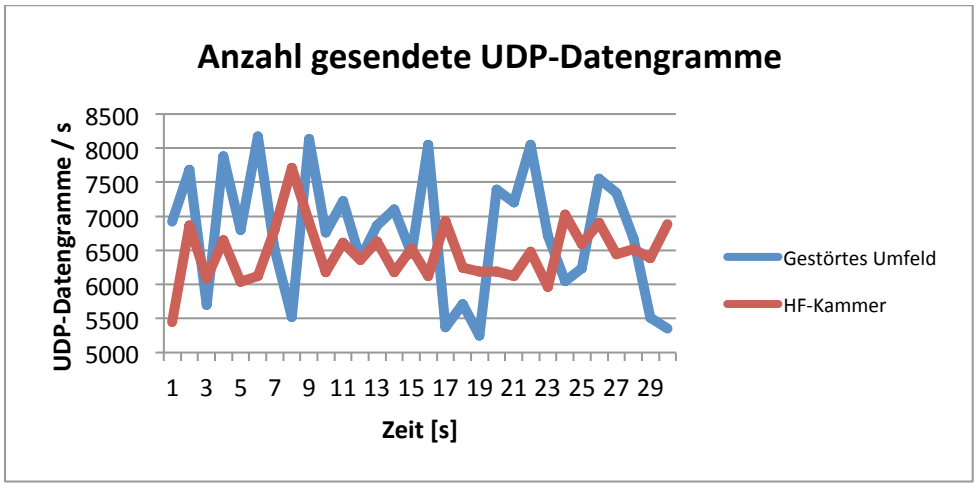

Anzahl verlorene UDP-Datengramme
Verlorene UDP-Datengramme
120
100
80
60
40
20
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29
Zeit [s]
Gestörtes Umfeld
HF-Kammer

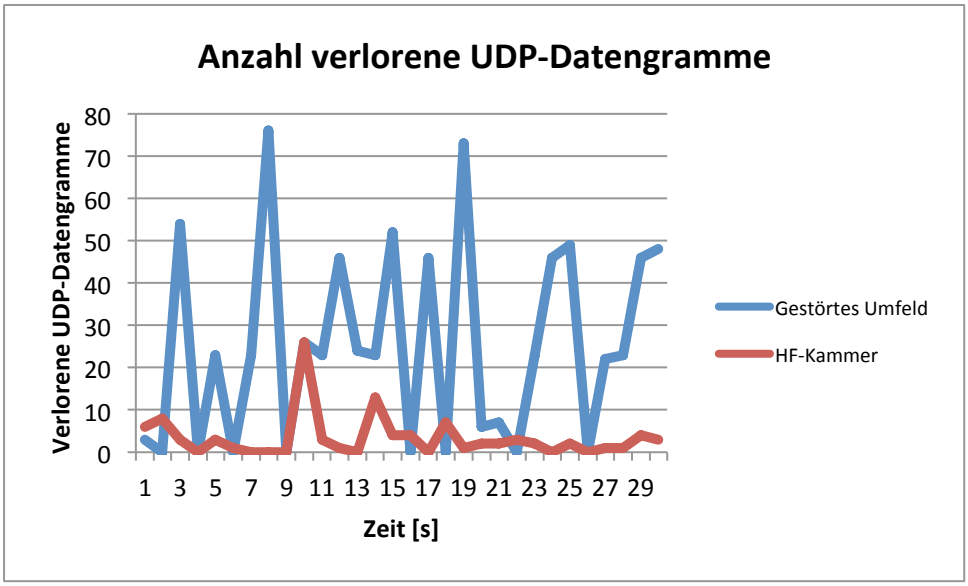
RIFS

20 MHZ KANALBREITE



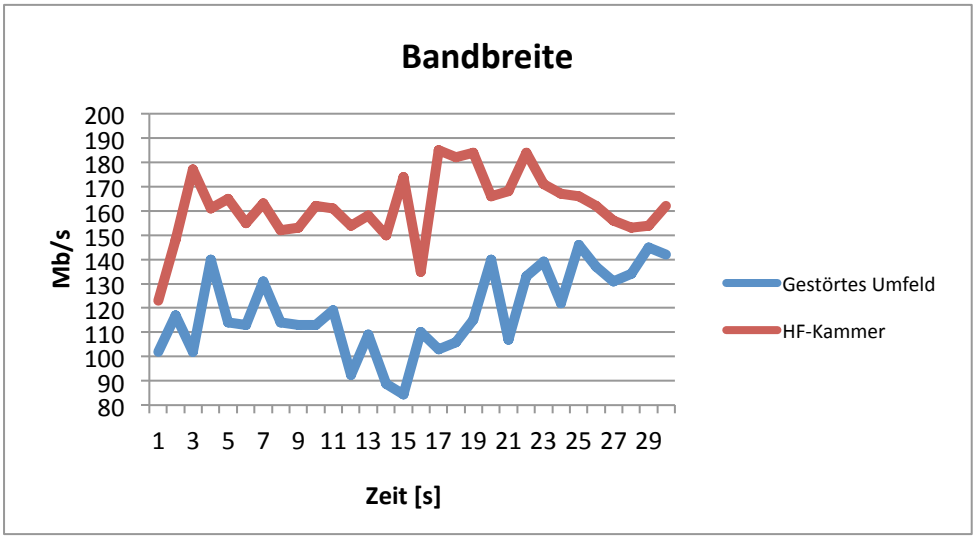


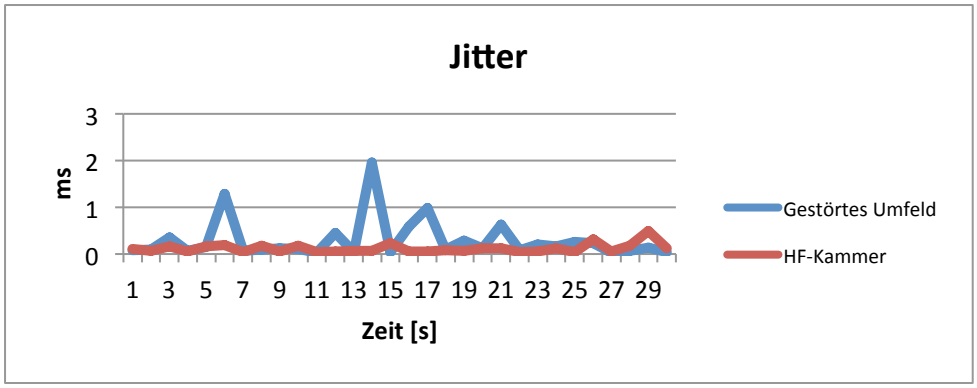


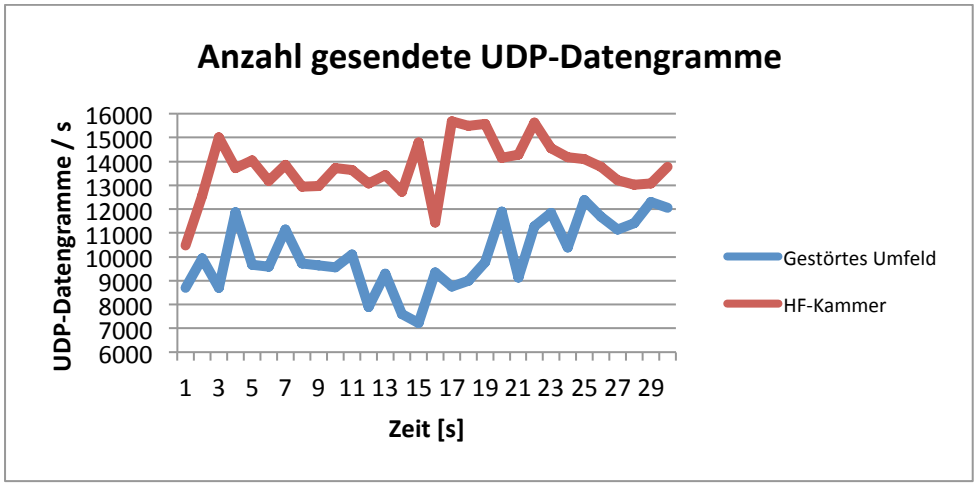


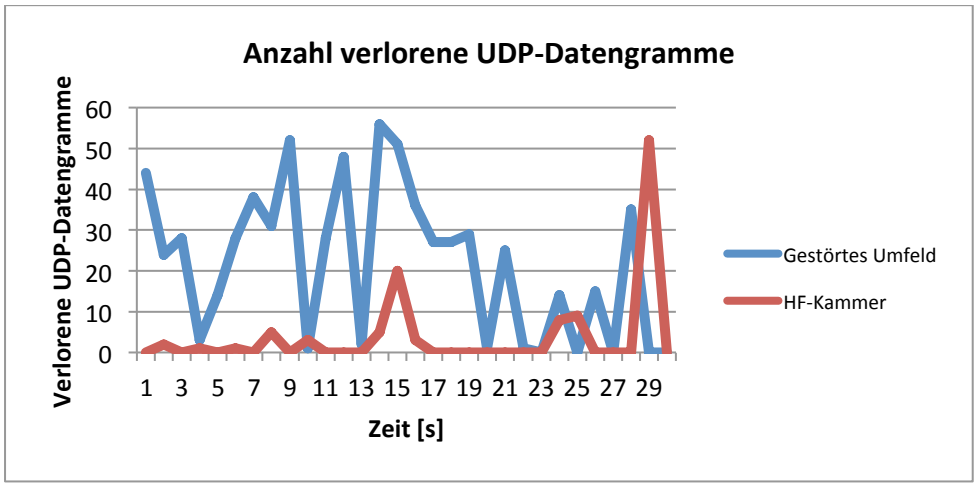
Bei der Verwendung von RIFS mit einer Kanalbreite von 20 MHz ist erkennbar, dass in der HF-Kammer deutlich weniger UDP-Datengramme gesendet wurden als im gestörten Umfeld. Dies führte dann auch zu einem geringeren Durchsatz. Hier liegt das Problem in der Verwendung der MIMO-Technologie, die in der HF-Kammer nicht funktioniert.

40 MHZ KANALBREITE









Bei RIFS mit einer Kanalbreite von 40 MHz zeigt sich, dass in der HF-Kammer wieder höhere Werte erreicht wurden als im gestörten Umfeld.

PERSÖNLICHER BERICHT

SELBSTREFLEXION

Ich habe bei dieser Arbeit positive als auch negative Erfahrungen gemacht. Zu den positiven Erfahrungen gehören sicher, dass ich jetzt ein breites Wissen im WLAN Bereich erarbeitet habe, das ich in meiner Tätigkeit im Netzwerkbereich anwenden kann. Zusätzlich habe ich gelernt, wie man Messungen vorbereitet, durchführt und analysiert. Positiv fand ich auch den Umgang mit Herrn Prof. Dr. Rinkel Andreas. Ich fand es gut, dass wir wöchentlich eine Sitzung durchgeführt haben, um dass weitere Vorgehen zu besprechen. Des Weiteren wurde ich von Herrn Rinkel motiviert, wenn ich einmal nicht weitergekommen bin, weil Probleme anstanden.

Was ich negativ empfunden habe und bei der nächsten Arbeit verbessern würde ist sicherlich der Zeitplan. Ich habe gemerkt, dass ich mich da verschätzt habe. Hier würde ich in Zukunft mehr Reservezeit für unvorhersehbares einplanen. Bei der Bearbeitung des G-Standards ist aufgefallen, dass eigentlich dazu auch der E-Standard eine wesentliche Rolle spielt. Aus diesem Grund habe ich noch den E-Standard gelesen, was einen Zeitaufwand von ungefähr 20h betrug. Dies war mir bei der Erstellung des Zeitplans nicht bewusst. Des Weiteren werde ich in Zukunft auch mehr Zeit bei der Auswertung von Messresultate einplanen. Auch hier hat sich gezeigt, dass ich mich verschätzt habe.

Eine weitere Anmerkung was ich bei der nächsten Arbeit verbessern werde ist dass ich Hardware, die ich während der Arbeit benötige, früher anfordere. Auch benötigte Räume würde ich einige Wochen vorher reservieren. Hier hatte ich Glück, dass alles immer geklappt hat.

LITERATURVERZEICHNIS

[1] Matthew Gast, “802.11 Wireless Networks: The Definitive Guide”, O’Reilly, April 2002.

[2] IEEE 802.11-2007, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, March 2007.

[3] IEEE 802.11e-2005, “Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements“, September 2005.

[4] IEEE 802.11n-2009, “ Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification“, October 2009.

[5] User Manual des Cisco Access Point WAP4410N ,

- http://www.cisco.com/en/US/products/ps10052/index.html, letzter Zugriff am 27.04.2012

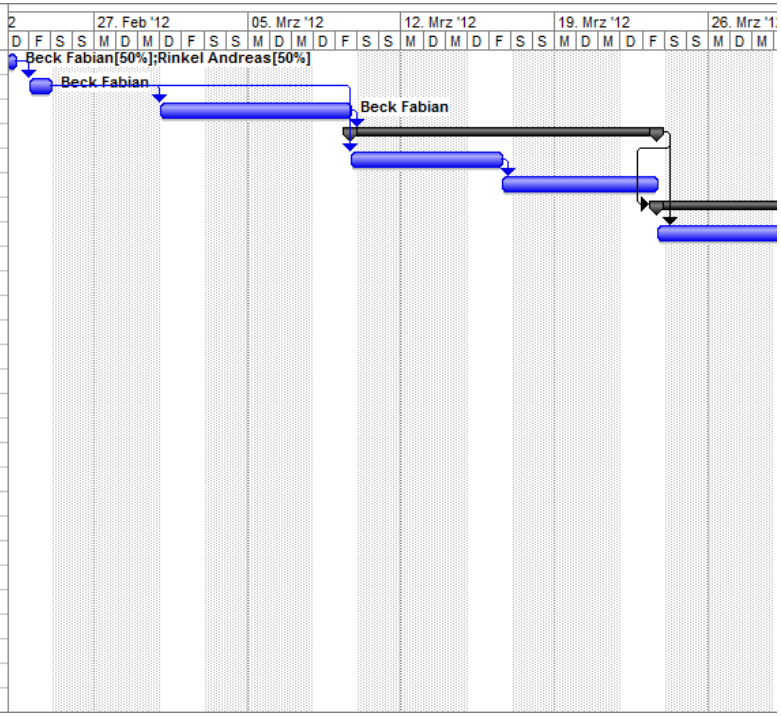
[6] User Manual des Netgear Access Point WNDAP350,

- http://support.netgear.com/app/products/model/a_id/12823, letzter Zugriff am 26.04.2012

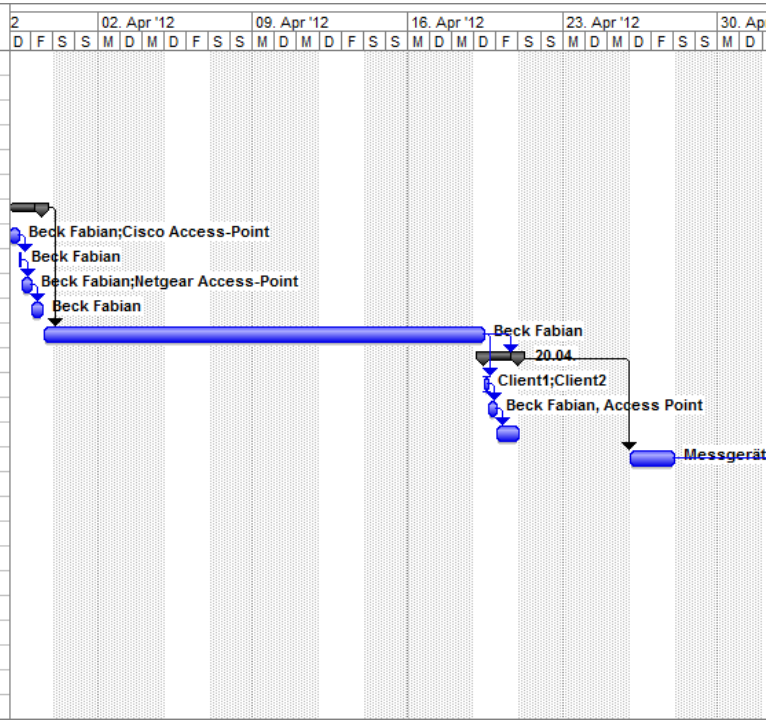
PROJEKTDOKUMENTE

PROJEKTMANAGEMENTPLAN

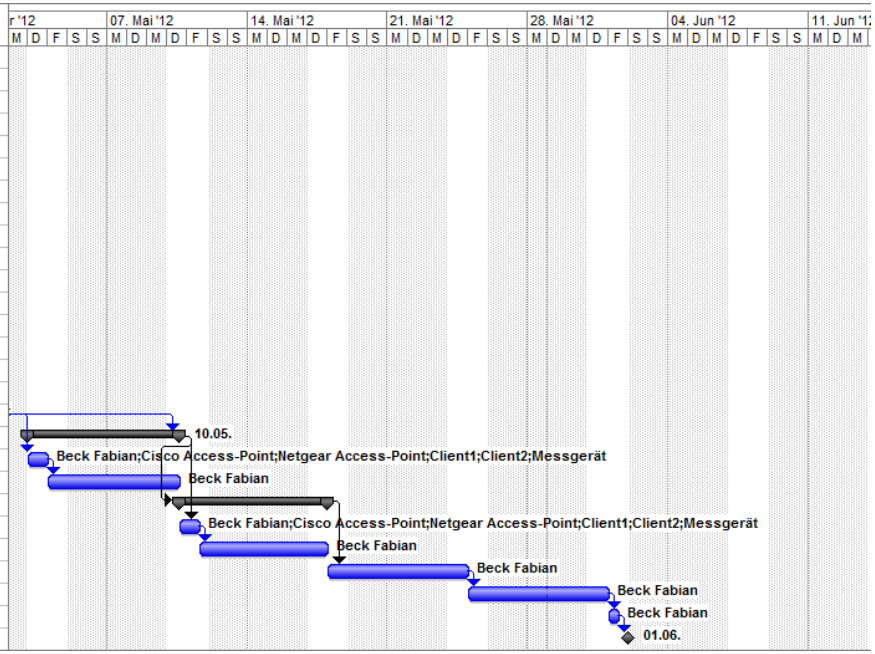
Nr.	Vorgangsname	Dauer	Anfang	Ende	Vorgänger
1	Projektstart	1 Std.	Do 23.02.12	Do 23.02.12	
2	Erstellen der Dokumente PMP und Risikoanalyse	8 Std.	Fr 24.02.12	Fr 24.02.12	1
3	Einlesen in die Theorie	35 Std.	Do 01.03.12	Fr 09.03.12	2
4	**Theorieteil schreiben**	**36 Std.**	**Fr 09.03.12**	**Fr 23.03.12**	**3**
5	WLAN Grundlagen (Infrastruktur, CSMA/CA, Frequenzen, Management Frames)	16 Std.	Fr 09.03.12	Fr 16.03.12	2
6	WLAN Standards beschreiben (IEEE 802.11 (g), (n) und (e))	20 Std.	Fr 16.03.12	Fr 23.03.12	5
7	**Kennenlernen der verwendeten Accesspoints**	**15 Std.**	**Fr 23.03.12**	**Fr 30.03.12**	**4**
8	Kennenlernen des Cisco AP's	3 Std.	Fr 23.03.12	Do 29.03.12	4
9	Beschreiben der Funktionen des Cisco AP's	3 Std.	Do 29.03.12	Do 29.03.12	8
10	Kennenlernen des Netgear AP's	5 Std.	Do 29.03.12	Do 29.03.12	9
11	Beschreiben der Funktionen des Netgear AP's	4 Std.	Fr 30.03.12	Fr 30.03.12	10
12	Messszenarien ausarbeiten (was / wie soll gemessen werden, theoretische Ergebnisse)	42 Std.	Fr 30.03.12	Do 19.04.12	7
13	**Vorbereitung der Messversuche**	**16 Std.**	**Do 19.04.12**	**Fr 20.04.12**	**12**
14	Konfiguration der Clients	4 Std.	Do 19.04.12	Do 19.04.12	12
15	Konfiguration der Access-Points	4 Std.	Do 19.04.12	Do 19.04.12	14
16	Dokumentation der Vorbereitung schreiben	8 Std.	Fr 20.04.12	Fr 20.04.12	15
17	Kennenlernen des Messgerätes inkl. dokumentieren	18 Std.	Do 26.04.12	Fr 27.04.12	13
18	**Messversuche im gestörten Umfeld**	**24 Std.**	**Do 03.05.12**	**Do 10.05.12**	**17**
19	Durchführung der Messszenarien	10 Std.	Do 03.05.12	Do 03.05.12	17
20	Dokumentation der Messergebnisse (Messprotokolle)	14 Std.	Fr 04.05.12	Do 10.05.12	19
21	**Messversuche im HF-Raum**	**22 Std.**	**Do 10.05.12**	**Do 17.05.12**	**18**
22	Durchführung der Messszenarien	10 Std.	Do 10.05.12	Fr 11.05.12	18
23	Dokumentation der Messergebnisse (Messprotokolle)	12 Std.	Fr 11.05.12	Do 17.05.12	22
24	Überprüfen der Dokumentation (Rechtschreibung, Vollständigkeit etc.)	18 Std.	Fr 18.05.12	Do 24.05.12	21
25	Reservezeit für unvorhersehrbares	18 Std.	Fr 25.05.12	Do 31.05.12	24
26	Selbstreflexion schreiben	4 Std.	Fr 01.06.12	Fr 01.06.12	25
27	Drucken, Binden und Abgabe der Arbeit an Herr Prof. Dr. Rinkel	4 Std.	Fr 01.06.12	Fr 01.06.12	26



Nr.	Vorgangsname	Dauer	Anfang	Ende	Vorgänger
1	Projektstart	1 Std.	Do 23.02.12	Do 23.02.12	
2	Erstellen der Dokumente PMP und Risikoanalyse	8 Std.	Fr 24.02.12	Fr 24.02.12	1
3	Einlesen in die Theorie	35 Std.	Do 01.03.12	Fr 09.03.12	2
4	**Theorieteil schreiben**	**36 Std.**	**Fr 09.03.12**	**Fr 23.03.12**	**3**
5	WLAN Grundlagen (Infrastruktur, CSMA/CA, Frequenzen, Management Frames)	16 Std.	Fr 09.03.12	Fr 16.03.12	2
6	WLAN Standards beschreiben (IEEE 802.11 (g), (n) und (e))	20 Std.	Fr 16.03.12	Fr 23.03.12	5
7	**Kennenlernen der verwendeten Accesspoints**	**15 Std.**	**Fr 23.03.12**	**Fr 30.03.12**	**4**
8	Kennenlernen des Cisco AP's	3 Std.	Fr 23.03.12	Do 29.03.12	4
9	Beschreiben der Funktionen des Cisco AP's	3 Std.	Do 29.03.12	Do 29.03.12	8
10	Kennenlernen des Netgear AP's	5 Std.	Do 29.03.12	Do 29.03.12	9
11	Beschreiben der Funktionen des Netgear AP's	4 Std.	Fr 30.03.12	Fr 30.03.12	10
12	Messszenarien ausarbeiten (was / wie soll gemessen werden, theoretische Ergebnisse)	42 Std.	Fr 30.03.12	Do 19.04.12	7
13	**Vorbereitung der Messversuche**	**16 Std.**	**Do 19.04.12**	**Fr 20.04.12**	**12**
14	Konfiguration der Clients	4 Std.	Do 19.04.12	Do 19.04.12	12
15	Konfiguration der Access-Points	4 Std.	Do 19.04.12	Do 19.04.12	14
16	Dokumentation der Vorbereitung schreiben	8 Std.	Fr 20.04.12	Fr 20.04.12	15
17	Kennenlernen des Messgerätes inkl. dokumentieren	18 Std.	Do 26.04.12	Fr 27.04.12	13
18	**Messversuche im gestörten Umfeld**	**24 Std.**	**Do 03.05.12**	**Do 10.05.12**	**17**
19	Durchführung der Messszenarien	10 Std.	Do 03.05.12	Do 03.05.12	17
20	Dokumentation der Messergebnisse (Messprotokolle)	14 Std.	Fr 04.05.12	Do 10.05.12	19
21	**Messversuche im HF-Raum**	**22 Std.**	**Do 10.05.12**	**Do 17.05.12**	**18**
22	Durchführung der Messszenarien	10 Std.	Do 10.05.12	Fr 11.05.12	18
23	Dokumentation der Messergebnisse (Messprotokolle)	12 Std.	Fr 11.05.12	Do 17.05.12	22
24	Überprüfen der Dokumentation (Rechtschreibung, Vollständigkeit etc.)	18 Std.	Fr 18.05.12	Do 24.05.12	21
25	Reservezeit für unvorhersehrbares	18 Std.	Fr 25.05.12	Do 31.05.12	24
26	Selbstreflexion schreiben	4 Std.	Fr 01.06.12	Fr 01.06.12	25
27	Drucken, Binden und Abgabe der Arbeit an Herr Prof. Dr. Rinkel	4 Std.	Fr 01.06.12	Fr 01.06.12	26



Nr.	Vorgangsname	Dauer	Anfang	Ende	Vorgänger
1	Projektstart	1 Std.	Do 23.02.12	Do 23.02.12	
2	Erstellen der Dokumente PMP und Risikoanalyse	8 Std.	Fr 24.02.12	Fr 24.02.12	1
3	Einlesen in die Theorie	35 Std.	Do 01.03.12	Fr 09.03.12	2
4	**Theorieteil schreiben**	**36 Std.**	**Fr 09.03.12**	**Fr 23.03.12**	**3**
5	WLAN Grundlagen (Infrastruktur, CSMA/CA, Frequenzen, Management Frames)	16 Std.	Fr 09.03.12	Fr 16.03.12	2
6	WLAN Standards beschreiben (IEEE 802.11 (g), (n) und (e))	20 Std.	Fr 16.03.12	Fr 23.03.12	5
7	**Kennenlernen der verwendeten Accesspoints**	**15 Std.**	**Fr 23.03.12**	**Fr 30.03.12**	**4**
8	Kennenlernen des Cisco AP's	3 Std.	Fr 23.03.12	Do 29.03.12	4
9	Beschreiben der Funktionen des Cisco AP's	3 Std.	Do 29.03.12	Do 29.03.12	8
10	Kennenlernen des Netgear AP's	5 Std.	Do 29.03.12	Do 29.03.12	9
11	Beschreiben der Funktionen des Netgear AP's	4 Std.	Fr 30.03.12	Fr 30.03.12	10
12	Messszenarien ausarbeiten (was / wie soll gemessen werden, theoretische Ergebnisse)	42 Std.	Fr 30.03.12	Do 19.04.12	7
13	**Vorbereitung der Messversuche**	**16 Std.**	**Do 19.04.12**	**Fr 20.04.12**	**12**
14	Konfiguration der Clients	4 Std.	Do 19.04.12	Do 19.04.12	12
15	Konfiguration der Access-Points	4 Std.	Do 19.04.12	Do 19.04.12	14
16	Dokumentation der Vorbereitung schreiben	8 Std.	Fr 20.04.12	Fr 20.04.12	15
17	Kennenlernen des Messgerätes inkl. dokumentieren	18 Std.	Do 26.04.12	Fr 27.04.12	13
18	**Messversuche im gestörten Umfeld**	**24 Std.**	**Do 03.05.12**	**Do 10.05.12**	**17**
19	Durchführung der Messszenarien	10 Std.	Do 03.05.12	Do 03.05.12	17
20	Dokumentation der Messergebnisse (Messprotokolle)	14 Std.	Fr 04.05.12	Do 10.05.12	19
21	**Messversuche im HF-Raum**	**22 Std.**	**Do 10.05.12**	**Do 17.05.12**	**18**
22	Durchführung der Messszenarien	10 Std.	Do 10.05.12	Fr 11.05.12	18
23	Dokumentation der Messergebnisse (Messprotokolle)	12 Std.	Fr 11.05.12	Do 17.05.12	22
24	Überprüfen der Dokumentation (Rechtschreibung, Vollständigkeit etc.)	18 Std.	Fr 18.05.12	Do 24.05.12	21
25	Reservezeit für unvorhersehrbares	18 Std.	Fr 25.05.12	Do 31.05.12	24
26	Selbstreflexion schreiben	4 Std.	Fr 01.06.12	Fr 01.06.12	25
27	Drucken, Binden und Abgabe der Arbeit an Herr Prof. Dr. Rinkel	4 Std.	Fr 01.06.12	Fr 01.06.12	26



RISIKOANALYSE

Risiko Bewertungen								
Risk ID	Risiko	Auswirkung	Massnahme	Kosten der Massnahmen in Zeit	Max. Schaden in h	Wahrschein-lichkeit des Eintreffens	Gewichteter Schaden in h	Priorität
R01	Access-Points werden gestohlen	Zeitverzögerung der SA	Access-Points in einem abschliessbaren Raum unterbringen	10 Min. / Woche	40	10%	4.00	mittel
R03	HF-Kammer kann zu den gewünschten Terminen nicht benutzt werden	Messungen in der HF-Kammer verzögern sich	Termine für HF-Kammer fix abmachen	1 mal 10 Minuten	40	5%	2.00	mittel
R04	Messgeräte kommen nicht zum gewünschten Zeitpunkt	Messungen verzögern sich	Termin zwei Wochen vorher der externen Firma bekanntgeben	30 Minuten	40	20%	8.00	hoch
R05	Ausfall des persönlichen Computers	Neuste Version der SA ist nicht mehr vorhanden	Tägliche Backups erstellen	5 Min. / Tag	10	15%	1.50	niedrig
R06	Fehleinschätzung des Aufwandes	Es entsteht mehr Arbeitszeit als geplant		-	40	15%	6.00	hoch
	Total Kosten in Arbeitspaketen enthalten(Angaben in h)			5				
	Total Rückstellungen				170		22	