ComConsult Research

Der Netzwerk Insider

Mai 2012

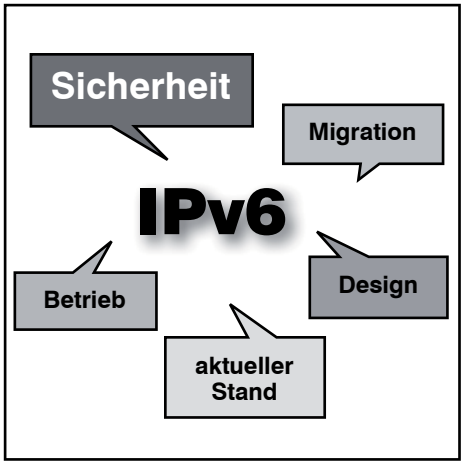
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

IPv6 und Sicherheit - wann, wie, und wo stehen wir?

von Dipl.-Inform. Oliver Flüs

IPv6 steht mindestens vor der Tür. Der Vorrat an Internet-tauglichen IPv4-Adressen geht nun tatsächlich langsam zur Neige, und es existieren konkrete Vorschläge, bis wann Internet-Service-Provider (ISPs) IPv6-Zugänge zum Internet anbieten sollen sowie Internet-Auftritte von öffentlichen Einrichtungen und Firmen (auch) unter IPv6 erreichbar sein sollten. Diese Ideen zum zeitlichen Verlauf haben ihren Ausgangspunkt bei einem Vorschlag der IETF (RFC 5211), der dann z.B. von der EU und im Rahmen des Aktionsplan des deutschen Rats für IPv6 (IPv6 Council) übernommen wurden.



Zwar hinkt die praktische Umsetzung diesen Plänen bereits ein wenig hinterher (Beispiel: IPv6-Angebote durch die Internet-Service-Provider waren bereits für 2011 vorgesehen). Jedoch ist aufgeschoben ja bekanntlich nicht aufgehoben, und die wichtigsten ISPs werden in absehbarer Zeit ihren Kunden die Möglichkeit anbieten, Internet-Präsenzen über IPv6 zugänglich zu machen bzw. zu nutzen.

weiter auf Seite 10

Zweitthema

Wireless LAN mit Gigabit-Geschwindigkeit

Herausforderung für Hersteller und Betreiber

von Dr. Joachim Wetzlar

Spätestens seit der Consumer Electronics Show (CES) im Januar dieses Jahres ist klar, dass es die Hersteller ernst meinen mit Gigabit-WLAN.

Mehrere Halbleiter-Produzenten haben Chipsätze für WLAN nach dem zukünftigen Standard IEEE 802.11ac vorgestellt, Geräte-Hersteller konnten bereits Prototypen von WLAN-Routern zeigen und damit Nutzlasten mit bis zu 800 Mbit/s übertragen – immerhin! Die Prototypen zielen zunächst auf den Consumer-Markt. Aber auch vor den professionellen WLANs wird diese Technik nicht Halt machen. Wir sollten uns also bereits jetzt schon mit der Technik vertraut machen und mit den Konsequenzen, die sich daraus für Planung und Betrieb von WLANs ergeben.

weiter auf Seite 21

Geleit

Wireless-Versorgungs-Strukturen: kommen die Hybriden?

auf Seite 2

Neuer Report - Subskriptionsphase

Cisco versus Microsoft: Wer hat die bessere Unified-Communications-Lösung?

auf Seite 19

Standpunkt

Das Schweizer Taschenmesser für den Netzbetrieb?

auf Seite 20

Aktuelle Kongress

ComConsult IT-Sicherheits-Forum 2012

ab Seite 5

Zum Geleit

Wireless-Versorgungs-Strukturen: kommen die Hybriden?

Die Messe für Mobilkommunikation in Barcelona und die letzten Quartalsergebnisse von Herstellern für Endgeräte, Chips und Infrastruktur sowie verschiedener Provider brachten nicht nur die Erkenntnis, dass die Backbone-Netze der Provider durch Fortschritte in der optischen Übertragungstechnik auch in Zukunft praktisch keine Limits zu befürchten haben, sondern auch eine erhebliche Verfestigung des 4G-Mobilfunk (LTE). Für ein Unternehmen ist die Frage der zukünftigen Gestaltung von Wireless-Versorgungs-Strukturen von elementarer Bedeutung. Neben dem klassischen WLAN und dem 4G Mobilfunk wird es noch eine weitere Alternative geben: hybride Access Points oder WLAN-Controller, die beide Welten beherrschen und zu neuen Planungsmöglichkeiten führen.

Spätestens seit der überaus erfolgreichen Einführung des iPad 3 durch Apple muss auch der Skeptiker einsehen, dass 4G nicht mehr zu bremsen ist. In einer Reihe von Märkten für das iPad 3 war 4G gar nicht oder nur sehr eingeschränkt verfügbar. Hier gab es sofort lautes Wehklagen und in Australien wollten Verbraucherschützer Apple wegen irreführender Werbung verklagen, was allerdings mit einer Entschädigung für die entsprechenden Käufer auf kurzem Wege geregelt werden konnte.

Weltweit rüsten Provider auf 4G-LTE um. Die bekanntesten Großprojekte kommen z. Zt. von Verizon und T-Mobile (USA). Die technischen Varianten sind dabei unterschiedlich, so wird China direkt mit der SCDMA-Variante ausgerüstet. Allgemein hat es sich durchgesetzt, neue Projekte auf der Basis von „LTE-Advanced"-Standardisierung der ITU vorzunehmen. LTE-Advanced (oder LTE 10) kann im Endausbau bis zu 1 Gbit/s. Up- und Downlink für eine individuelle Subscriber Station liefern. Aktuell sind Datenraten von 84 und 150 Mbit/s.

Eine Schlüsselrolle bei der aktuellen Entwicklung spielt der Chip-Hersteller Qualcomm. Dieser Hersteller hat die meisten Patente für LTE und ist Hoflieferant von Apple für die Kommunikationschips. Qualcomm konnte Umsatz und Gewinn im letzten Quartal erheblich steigern, hat aber jetzt das „Luxusproblem", dass sie den Bedarf von Apple nicht so schnell

decken können, wie Apple das möchte. Denn unbemerkt von den Meisten vollzieht sich auch bei den Funkchips ein Wechsel von der bisherigen 45 nm-Technologie zur 28 nm-Technologie. Dieser Wechsel bedeutet nicht nur einen niedrigeren Energiebedarf, sondern auch eine erhebliche Zunahme der auf einem Chip möglichen Funktionen. Es ist natürlich klar, dass Apple und andere Hersteller jetzt nur noch mit den neuen Chips planen möchten. Der Aufbau der entsprechenden Produktions-Kapazitäten ist jedoch nicht so einfach und auch in gewisser Weise riskant. Hersteller von SSD-Chips haben z.B. im letzten Quartal schmerzliche Erfahrungen mit Überkapazitäten gemacht, die der Markt nicht so schnell aufnehmen konnte.

Wie so oft ist es ein einziger Chip, der zu einer kleinen Revolution führt. Der MDM 9615 von Qualcomm ist ein „2G – 4G"-Universalchip und beherrscht LTE-TDD, LTE-SCDMA, FDD, CDMA, WCDMA und GSM. Mit Multi-Band und Carrier-Aggregation deckt er praktisch den gesamten Bereich statistisch wichtiger Mobilfunktechniken von 2G bis HSPA+ (LTE Rel.10) ab. Das ist für Endgeräte-Hersteller eine Rettung vor teuren Diversifizierungen im Hinblick auf regionale Teilmärkte und für Provider sehr praktisch, da sie ihre Netze in der gebotenen Ruhe weiterentwickeln können. In einem Endgerät benötigt man zu diesem Chip zwingend noch einen Radio-IC und optional einen weiteren für das Power-Management. Der Chip hat auch einen eigenen Kosenamen: „Gobi-Chip", wahrscheinlich weil er die Konkurrenz in die Wüste schicken soll. Als Maximal-Leistung für eine Verbindung gibt der Hersteller 150 Mbit/s. an.

Die seit einigen Wochen z.B. in den USA ausgelieferten iPad 3 haben noch einen 45nm 4G-Chip. Der MDM 9615 wird erst im 3Q12 in Stückzahl verfügbar sein. Deshalb erwartet man auch das iPhone 5 erst zu diesem Zeitpunkt. Dann wird es auch nochmal ein für den Weltmarkt überarbeitetes iPad mit universellen 4G-Fähigkeiten geben, nennen wir es jetzt einfach mal iPad 3S.

Auch wenn hier vorwiegend die Produkte von Apple genannt werden, wird es natürlich auch von anderen Herstellern Pads und Smartphones geben, die die neuen Chips beinhalten und eben mit Android oder einem System von Microsoft betrieben werden.

Für ein Unternehmen stellt sich angesichts derartiger Entwicklungen natürlich die Frage, wie eine Wireless-Versorgungsstruktur gestaltet werden kann. Und da gibt es jetzt nicht nur zwei, sondern drei grundsätzliche Alternativen, die jeweils eine Reihe möglicher Ausprägungen nach sich ziehen:

1. Unternehmenseigene WLAN-Infrastruktur
2. (Reine) LTE-Infrastruktur
3. Hybride Infrastruktur

Unternehmenseigene WLAN-Infrastruktur

Das ist die Form, die heute überwiegend benutzt wird. In Abbildung 1 sehen wir die klassischen Komponenten. Heutige WLANs basieren vorwiegend auf 802.11n, Nachfolgestandards sind die bereits hinlänglich besprochenen Systeme nach IEEE 802.11ac und 802.11ad. 11ac wird eine sanfte Migration ermöglichen, weil es technisch erhebliche Parallelen zu 11n hat. Von daher bedarf vor allem die Zellenplanung keiner wesentlichen Änderungen. Die Leistung steigt zwar, aber nur um den Faktor 2-3 gegenüber 11n, alle anderen Versprechen können wir in Ruhe abwarten. Eine wirkliche Verbesserung hinsichtlich der Leistung steht bei 11ad zu erwarten. Funknetze im Millimeterwellenbereich gehorchen aber ganz anderen Randbedingungen. Die Zellen werden viel kleiner sein, daher wird es viel mehr Zellen geben müssen und genau das ist ein mögliches schwerwiegendes Problem für die hin-

Schwerpunkthema

IPv6-Adresse: die Qual der Wahl

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen Services im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig, unter anderem als Schwerpunktreferent zu TCP/IP-Aspekten, in der Trouble Shooter-Seminarreihe sowie im Rahmen der Sicherheitsseminare.

Auch die Produkthersteller haben das Thema IPv6 angenommen. Microsoft hat IPv6 gar zum „strategischen Teil“ seiner Betriebssystem-Produkte erklärt, Hersteller von Netzkomponenten wie z.B. Cisco bieten IPv6-Unterstützung im Rahmen aktueller Firmware-Versionen zu diversen Produkten an, und auch im Bereich der Anwendungen gibt es erste Beispiele von IPv6-Unterstützung. Zwar kann bei genauerer Betrachtung der IPv6-Unterstützung noch längst nicht davon gesprochen werden, dass für eine Ablösung von IPv4 durch IPv6 die notwendigen Produktverfügbarkeiten gegeben sind. Jedoch ist der Knoten „geplatzt“, das gegenseitige Warten von Produktherstellern, deren Kunden und der ISPs darauf, wer die notwendige Initiative ergreift, ist beendet.

Sofern nun eine neue Protokollbasis sich anschickt, in die eigene IT-Ausstattung Einzug zu halten, muss natürlich auch das Thema Sicherheit betrachtet werden. Allerdings – wenn doch bislang bei ISPs und Produktherstellern erst „Aufbruchstimmung“ bzgl. IPv6 herrscht, aber noch kein umfassendes Angebot besteht, lohnt sich dann eine Beschäftigung mit IPv6 unter Security-Gesichtspunkten zum jetzigen Zeitpunkt? Naheliegender mag erscheinen, das Thema IPv6 und damit auch IPv6-Sicherheit noch ein wenig auszusitzen und eine Beobachterposition einzunehmen. Wenn ein umfassendes IPv6-Produktangebot besteht, könnte man dann eine Einführung planen und dabei natürlich auch eine IPv6-Sicherheitskonzeption erstellen. Bis dahin gilt der typische Ansatz – was nicht eingesetzt werden soll, wird nicht installiert bzw. abgeschaltet!?

So einfach ist die Situation aber nicht.

Warum dies so ist, mit welchen Besonderheiten einer Übergangssituation auf dem Weg zu IPv6-basierten Umgebungen man aus Security-Sicht umgehen muss und wie man dabei vermeidet, sich über scheinbar plausible „einfache“ Sicherheitsstrategien unpraktikable Ziele zu setzen, soll im Folgenden mit Hilfe praxisnaher Überlegungen beleuchtet werden.

1. IPv6 – aber sicher!?

Sobald man eine Einführung von IPv6 plant, müssen auch Sicherheitskonzepte mit Blick hierauf überprüft und ergänzt werden. Neue Protokolle, auch wenn sie wie im Falle von IP einen wohlbekannten Vorgänger haben, bringen Details mit, die zumindest auf Ansätze für Sicherheitsangriffe und Möglichkeiten zur Erschwerung solcher Angriffe zu prüfen sind.

Warum sollte man sich aber bereits zum heutigen Zeitpunkt mit dem Thema „IPv6 und Sicherheit“ beschäftigen? Hier sind verschiedene Gründe zu sehen:

1.1 Vorbereitung einer IPv6-basierten Web-Präsenz als erste Aufgabe

Mit der Zeit werden erste Internet-Nutzer auf reine IPv6-basierte Kommunikation eingerichtet sein. Wer ihnen nur eine weiterhin ausschließlich über IPv4 ansprechbare Web-Präsenz anbieten kann, erzwingt die Nutzung von Übergangstechniken zur Verbindung von IPv4 und IPv6. Die damit verbundene Umsetzung zwischen den Protokollen bringt zusätzliche Laufzeitelemente mit sich, die bei langen Wegen zwischen Internet-Nutzer und Web-Auftritt zu Antwortzeiten führen können, die dem Nutzer unangenehm auffallen. Dies erhöht nicht gerade die Werbewirksamkeit der Web-Präsenz oder gar die Akzeptanz von Angeboten wie e-Business.

Irgendwo muss man mit IPv6 anfangen, warum also nicht im Bereich der Web-Anbindung? Die Anzahl der zu unterstützenden Dienste und Anwendungsformen ist übersichtlich, und erste Erfahrung mit IPv6-basierter Kommunikation kann helfen, die nachfolgende schrittweise Einführung der neuen Protokollversion auch für wichtige produktive Lösungen zu erleichtern und mit möglichst wenig Pannen zu überstehen – oder aber mit solchen Pannen geschickter umzugehen als ohne jegliche Einsatzerfahrung.

1.2 Herstellerverhalten und seine Auswirkung auf IPv6-Sicherheit

Jetzt, nachdem die Notwendigkeit eines mittelfristigen Einstiegs in IPv6 akut geworden ist, hat auch die Portierung von Produkten auf IPv6-Fähigkeit begonnen. Bei bereits am Markt erfolgreichen Produkten bedeutet dies zunächst, diese auch unter IPv6 nutzbar zu machen.

Bei neuen Produktentwicklungen kann es dann jedoch auch vorkommen, dass mit IPv6 neue technische Möglichkeiten bestehen, die erstens von jedem IPv6-fähigen Gerät unterstützt werden, und/oder zweitens dem Hersteller eines Produkts Antworten auf Fragen geben, die unter IPv4 nicht oder nicht zufriedenstellend zur Verfügung stehen.

Microsoft Direct Access ist ein erstes Beispiel für ein Produkt, das aus solchen Gründen sogar gezielt sofort auf Basis von IPv6 entwickelt und angeboten wird: Der Hersteller macht sich zunutze, dass IPv6 Authentication Header und Encapsulated Security Payload (ESP) als von jedem IPv6-Stack zu unterstützende optionale IP-Header mitbringt. Statt als Security-Basis eine eigene IPSec-artige Implementierung schaffen zu müssen, nutzt Microsoft die IPSec-Unterstützung durch die IPv6-Spezifikationen und Implementierungen.

Die IETF verhält sich übrigens schon eine Weile so: zu aktuellen Themen konzentriert man sich bei Internet-Drafts und RFCs mittlerweile auf IPv6-basierte Ansätze.

Wurden in der Vergangenheit mangels Verfügbarkeit IPv6-basierter Betriebssystemversionen dann doch noch IPv4-Ableger solcher Ideen gezogen, so sollte man in Zukunft hierauf nicht spekulieren. Warum sollten noch Spezifikationen zu Ansätzen auf einer IPv4-Basis geschaffen werden, die doch eine aussterbende Plattform darstellt - wo doch jetzt die Möglichkeit zur Nutzung der Nachfolgeversion IPv6 auch produkteseitig aufgebaut wird?

Weitere mögliche Gründe, aus denen ein Hersteller früher oder später mit Konsequenz in IPv6-basierte Produktimplementierung einsteigen wird, sind etwa

- Belieferung von Märkten mit akuter Knappheit an IPv4-Adressen
- Neue „Produktideen“ mit massivem Bedarf an „öffentlichen“ IP-Adressen

  Ein häufiger ins Gespräch gebrachtes Thema ist hier z.B. „Smart Grids“/ intelligentes Stromnetz. Stromerzeugung, Stromspeicherung, Übertragung und Verbraucher sollen hier so vernetzt werden, dass durch den entstehenden Informationsfluss auf den jeweils aktuellen Bedarf reagiert werden kann.

Je mehr auf Grund solcher Überlegungen Hersteller in IPv6-basierte Lösungen investieren, umso mehr wird sich aus Herstellersicht die Priorität verändern. Bietet man ein Produkt IPv4- und IPv6-basiert an und tut dies gleichwertig, so kann der Käufer auch erwarten, dass beide Nutzungsvarianten gleichartig betreut werden (Tests bis zur Produktreife, Support). Dies bedeutet erhöhte Kosten beim Hersteller. Die übliche Konsequenz in solchen Fällen: Hält ein Hersteller seine neue, neueste technische Spezifikationen nutzende Lösung für ausreichend stabil und ausgereift, so macht er die Nutzung der älteren Alternativen schrittweise unattraktiv, um den Aufwand für Pflege und Betreuung dieser älteren Ansätze abbauen zu können.

Die IETF empfiehlt IPv6 – der Hersteller zieht (über kurz oder lang) mit

Hinzu kommt: Die IETF fordert sogar, Hersteller sollen aufhören, IPv6 als optional zu betrachten, und auf eine Produktentwicklung unter Konzentration auf IPv6 einschwenken, siehe RFC 6540 (Kategorie: Best Current Practices):

```
To ensure interoperability and flexibility, the best practices are as
follows:

o  New IP implementations must support IPv6.

o  Updates to current IP implementations should support IPv6.

o  IPv6 support must be equivalent or better in quality and
   functionality when compared to IPv4 support in a new or updated IP
   implementation.

o  New and updated IP networking implementations should support IPv4
   and IPv6 coexistence (dual-stack), but must not require IPv4 for
   proper and complete function.

o  Implementers are encouraged to update existing hardware and
   software to enable IPv6 wherever technically feasible.
```

1.3 Verzicht auf IPv6 bis zur Einführungsentscheidung – Machbarkeit?!

Deaktivierung von IPv6 als vorläufige Härtungsentscheidung?

Erste Konsequenzen solcher Entwicklungen bei der Herstellerstrategie können dann so aussehen, dass von neuen Produktversionen auch das Vorhandensein neuester Protokollbasis (hier eben: IPv6) als Installationsgrundlage vorausgesetzt wird.

So hat beispielsweise Microsoft für die neuesten Windows-Versionen formuliert, dass IPv6 als verbindlicher Teil des Betriebssystems betrachtet werde und dass Tests im Rahmen der Produktentwicklung mit aktiviertem IPv6 erfolgen (siehe etwa http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx - Abschnitt „The Argument against Disabling IPv6“). Anders herum betrachtet bedeutet dies: Wer unter neuesten Windows-Versionen IPv6 deaktiviert, tut dies „auf eigene Gefahr“ bzgl. schädlicher Seiteneffekte. Dabei verhält sich Microsoft hier nur vorbildlich im Sinne der oben zitierten IETF-Forderung.Manöverkritik am Hersteller ist daher wenig angebracht und auch nicht hilfreich.

Kann also IPv6 im Sinne einer entsprechenden vorläufigen Härtungsstrategie auf einem Windows-System konsequent deaktiviert werden, ohne dass dies Seiteneffekte auf Stabilität oder Lauffähigkeit der Dienste und Anwendungen hat? (Es hat bereits erste praxisrelevante Gegenbeispiele gegeben, z.B. Microsoft Exchange-Installationen, die ohne Aktivierung von IPv6 nicht starten.) Ist es praktikabel, entsprechende Tests vorbereitend durch zuführen?

Wenn nicht, ist der Härtungsansatz „IPv6 ist abzuschalten“ nicht länger durchgängig praktikabel!

Verzicht auf IPv6-fähige Produktversionen als vorläufiger Sicherheitsansatz?

Zudem soll gemäß den oben zitierten RFC-Forderungen die IPv6-Unterstützung gleichwertig wie oder in Qualität und Funktionalität besser sein als die IPv4-Unterstützung. Dies kann bei konsequenter Umsetzung in der Produktpflege im Extremfall auch dazu führen, dass stabilisierende Updates zuerst (oder gar ausschließlich) für die IPv6-basierte Nutzungsvariante zur Verfügung gestellt werden.

Als Nächstes kündigt ein Hersteller den Support für Versionen seiner Produkte ab, die noch kein IPv6 unterstützen bzw. benötigen. Sofort rückt das nächste sicherheitsrelevante Argument in den Vordergrund, das dann zu einem Einstieg in IPv6-basierte Produktversionen zwingen kann:

Wie lange kann man das Restrisiko tragen, durch Einsatz von Produktversionen ohne Hersteller-Support die Einführung IPv6-fähiger Produkte hinauszuzögern?

2. IPv6 ist womöglich schon da – zumindest „auf dem Rechner …“

Mit neueren Windows-Betriebssystemen (Vista / Windows 7, Windows Server 2008 und 2008 R2) hat man sogar Produkte, die mehr als nur laut an die Tür klopfen und dabei IPv6 als integriertes Element mitbringen, auf dessen Installation nicht verzichtet werden kann.

Der vom Hersteller im Zuge seiner strategischen Unterstützung von IPv6 gewählte Dual-Layer-Ansatz bedeutet, dass dieselbe IP-Software über dieselbe Schnittstelle zu Anwendungen und Diensten je nach Bedarf Kommunikation via IPv4 oder IPv6 realisiert. Wer diese Software und damit IPv6 beim Installieren weglassen wollte, hätte gar keine IP-Unterstützung mehr.

Zweitthema

Wireless LAN mit Gigabit-Geschwindigkeit - Herausforderung für Hersteller und Betreiber

Dr.-Ing. Joachim Wetzlar ist seit fast 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH. Er leitet dort das Competence Center „Trouble-Shooting und Messtechnik“ und ist maßgeblich an seinem Aufbau beteiligt. Er blickt auf einen erheblichen Erfahrungsschatz mit Messgeräten und den Details der Kommunikations-Protokolle zurück. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netz-Redesigns und WLAN-Planungen durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten Referenten mit hohem Praxisbezug.

Fortsetzung von Seite 1

Moment mal, die Hersteller entwickeln Chipsätze und Geräte für eine Technik, die noch gar nicht standardisiert ist? Im Grunde ist das ein gutes Zeichen. Einen erfolgreichen Standard erkennt man nämlich unter anderem daran, dass es Produkte bereits vor dessen Ratifizierung und Veröffentlichung gibt. Das war bei Gigabit Ethernet so, beim „High Througput“ WLAN (IEEE 802.11n) nicht anders und es wird auch auf das „Very High Throughput“ WLAN zutreffen, das jetzt in der Entstehung ist. Das Standardisierungsgremium, die „Task Group ac“ (TGac) bei IEEE 802.11 hat sich bereits in 2008 formiert. Zu diesem Zeitpunkt war 11n noch nicht einmal verabschiedet. Seit Juni 2011 liegt ein erster Draft vor, im Februar 2012 hat die TGac den zweiten Draft veröffentlicht. Die derzeitige Planung geht davon aus, dass man Ende 2013 einen fertigen Standard vorlegen kann.

Parallel dazu wird noch ein zweiter Standard entwickelt, der sich mit Gigabit-WLAN beschäftigt. Die „Task Group ad“ (TGad) wurde etwa zeitgleich zur TGac ins Leben gerufen. Sie beschäftigt sich mit einer völlig neuen Technik, die wesentlich höhere Frequenzen nutzt als es die bisherigen WLAN machen. Im Frequenzbereich um 60 GHz - das entspricht einer Wellenlänge von nur 5 Millimetern - lassen sich mit Leichtigkeit hohe Bitraten übertragen, weil man massenhaft Bandbreite zur Verfügung hat. Und man braucht sich nicht um die Kompatibilität mit der bestehenden Technik zu scheren. Dementsprechend schnell schreitet die TGad voran. Bereits im Oktober 2010 lag der erste Draft vor, im Oktober 2011 schon der fünfte.

Leider sind Produkte für diese Technik bisher nicht über ein Experimentalstadium hinausgekommen. Davon abgesehen weiß man bereits heute, dass sich mit 5-Millimeterwellen wohl Wände kaum durchdringen werden lassen. WLAN gemäß IEEE 802.11ad wird also immer nur punktuell eingesetzt werden können, etwa im Heimbereich oder in Büroumgebungen. Dass allerdings die Dämpfung durch Sauerstoff auf WLAN bei 60 GHz einen merklichen Einfluss haben wird, ist eine Mär. In der Tat ist die Dämpfung in diesem Frequenzbereich besonders hoch. Sie liegt in der Größenordnung von 10 bis 15 dB/km. Bezogen auf die bei WLAN typischen Abstände zwischen Access Point und mobilen Stationen ist das aber wohl irrelevant.

Ein flächendeckendes WLAN lässt sich also im 60-GHz-Band kaum aufbauen. Stattdessen wird man diese Technik dazu nutzen, ein vorhandenes WLAN „alter“ Technik punktuell zu ergänzen. Endgeräte werden also beide Techniken an Bord haben, um transparent zwischen den Frequenzbereichen umschalten zu können.

Demgegenüber sind WLANs gem. IEEE 802.11ac sozusagen eine Erweiterung der heute verbreiteten WLAN-Technik auf Frequenzen bei 2,4 und 5 GHz. Erstere sind allerdings für 11ac nicht wirklich zu gebrauchen, wie wir später sehen werden. Im 5-GHz-Band dagegen lassen sich prinzipiell Datenraten von (brutto) bis zu 7 Gbit/s erzielen. Wie funktioniert das?

Lassen Sie uns zunächst einen Blick auf das Ihnen bereits vertraute WLAN gem. IEEE 802.11a werfen. Es nutzt auch das 5-GHz-Band und stellt Brutto-Bitraten von bis zu 54 Mbit/s bereit. Genau genommen wird die verwendete Bitrate an die tatsächlichen Umgebungsbedingungen angepasst. Umgebung in diesem Sinne ist einerseits die Strecke zwischen Sender und Empfänger, die immer einer gewissen Dämpfung unterworfen ist. Die Dämpfung hängt von verschiedenen Faktoren ab, die wichtigsten sind die Entfernung und Hindernisse, wie beispielsweise Wände. Darüber hinaus können Funkstörungen die Empfangsbedingungen verschlechtern.

Der Sender kann nun verschiedene Parameter wählen, um entweder die Übertragungsrate zu erhöhen oder aber die Immunität gegen Störungen. Beides gleichzeitig geht nicht. Eine hohe Immunität gegen Störungen bedingt immer eine geringe Übertragungsrate. Parameter, die der Sender anpasst - und auf die sich der Empfänger natürlich einstellt - sind bei 11a:

- Das Modulationsverfahren: Es können vier verschiedene Verfahren gewählt werden. Das „langsamste“ und somit störsicherste ist die binäre Phasenmodulation (Binary Phase Shift Keying, BPSK), mit der sich ein Bit pro Zeiteinheit übertragen lässt. Das schnellste Verfahren ist eine Quadratur-Amplitudenmodulation, bei der sich 6 Bits pro Zeiteinheit kodieren lassen. Da sich mit 6 Bits 64 Werte darstellen lassen, heißt dieses Verfahren 64-QAM. Abbildung 1 zeigt die bei BPSK und 64-QAM möglichen Kombinationen aus Phasenwinkel und Amplitude (die bei 11ac mögliche Modulationsart 256-QAM ist auch dargestellt, dazu aber später). Das Problem wird sichtbar. Je enger die Punkte beieinander liegen, desto schwerer wird es für einen Empfänger, diese zu unterscheiden. Nebenbei bemerkt: Diese Art der unabhängigen Modulation zweier um 90 Grad phasenverschobener Trägersignale wurde im großen Stil erstmals bei der Farbfernsehtechnik eingesetzt, um die so genannten Farbdifferenzsignale zu übertragen. Stellt man die möglichen Kombinationen der

Wireless LAN mit Gigabit-Geschwindigkeit - Herausforderung für Hersteller und Betreiber

Amplitudenwerte beider Träger in einem rechtwinkligen Koordinatensystem dar, ergibt sich ein Quadrat – daher der Name.

- Der Faltungscode: Dabei handelt es sich um ein Verfahren, das sozusagen Redundanz in den Datenstrom hineincodiert. Wenn einzelne Bits durch Störungen verloren gehen, kann der Empfänger sie dank Redundanz wiederherstellen. Es ist offensichtlich, dass diese Redundanz zusätzliche Information ist, die übertragen werden muss. Als Code-Rate bezeichnet man nun den Anteil der Nutzdaten am Gesamt-Datenaufkommen. Code-Rate 3/4 bedeutet also, dass 75% des übertragenen Datenvolumens Nutzdaten sind, und die Redundanz also die verbleibenden 25% ausmacht. Ursprünglich, also bei 11a-WLAN, gibt es die Code-Raten 1/2, 2/3 und 3/4.

Vier verschiedene Modulationsverfahren und drei Code-Raten werden bei 11a zu 8 Bitraten zwischen 6 Mbit/s und 54 Mbit/s kombiniert. Die tatsächlich verwendete Kombination richtet sich danach, ob der Empfänger ein Paket empfangen hat. Das bestätigt er nämlich dem Sender. Bleibt diese Bestätigung aus, wird der Sender das Paket wiederholen und dabei eine Kombination mit geringerer Anfälligkeit gegen Störungen wählen; die Datenrate sinkt.

Die Entwickler des Standards IEEE 802.11n haben zunächst die von mir beschriebene Technik etwas „aufgebohrt". Es kam eine zusätzliche Code-Rate mit dem Wert 5/6 hinzu. Durch diese Maßnahme und weitere Optimierungen am Übertragungs- und Medienzugangsverfahren lässt sich die verfügbare Bitrate auf 72 Mbit/s steigern. Das ist noch kein großer Wurf. Ein großer Schritt in Richtung höherer Datenraten wird in 11n erst durch zwei neue Techniken erzielt. Das sind:

- Verdoppelung der Kanalbandbreite von 20 auf 40 MHz: Dadurch wird die Bitrate um 108% auf 150 Mbit/s erhöht. Wie geht das? Doppelte Bandbreite aber mehr als doppelt so viel Bitrate? Ganz einfach: Dadurch, dass zwei nebeneinander liegende Kanäle verwendet werden, lässt sich der „Zwischenraum", der normalerweise Nachbarkanalstörungen vermeidet, gleich mitverwenden. Das ist in Abbildung 2 angedeutet.

- Multiple Input Multiple Output (MIMO): Aus der Sicht eines mit der analogen Funktechnik vertrauten Menschen grenzt das an Zauberei. Es werden mehrere Sender verwendet, die auf derselben Frequenz unterschiedliche Signale aussenden. Auf der Empfänger-Seite mischen sich diese Signale und sind eigentlich nicht mehr voneinander zu trennen. Wenn aber der Empfänger ebenfalls mehrere Antennen einsetzt, wird er an jeder Antenne eine etwas andere Mischung der Sendesignale empfangen. Und diese Tatsache ermöglicht es Signalprozessoren, die Sendesignale bzw. deren Informationsgehalte wiederherzustellen (vgl. Abbildung 3). Die einzelnen Sendesignale werden auch als „Spatial Streams", zu Deutsch etwa „räumlich verteilte Datenströme" bezeichnet. Die Übertragung gelingt übrigens nur, wenn sich die Sendesignale auf möglichst unterschiedlichen Wegen zum Empfänger bewegen. Somit ist MIMO eine Technik, die für den Indoor-Einsatz mit seinen zahlreichen Reflexionsmöglichkeiten prädestiniert ist.

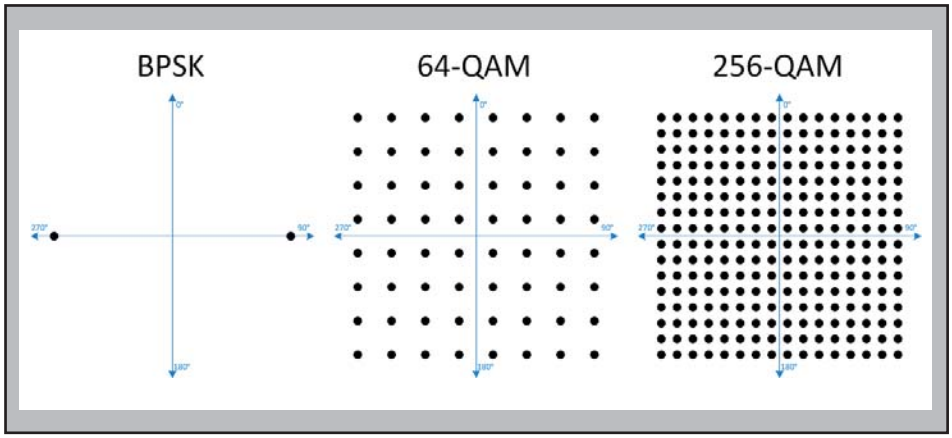


Abbildung 1: Gegenüberstellung einiger bei WLAN verwendeter Modulationsverfahren

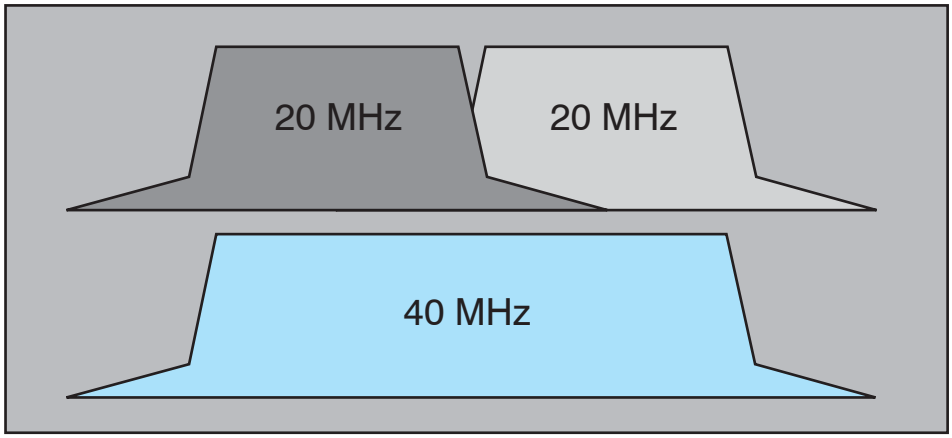


Abbildung 2: Verdoppelung der Kanalbandbreite

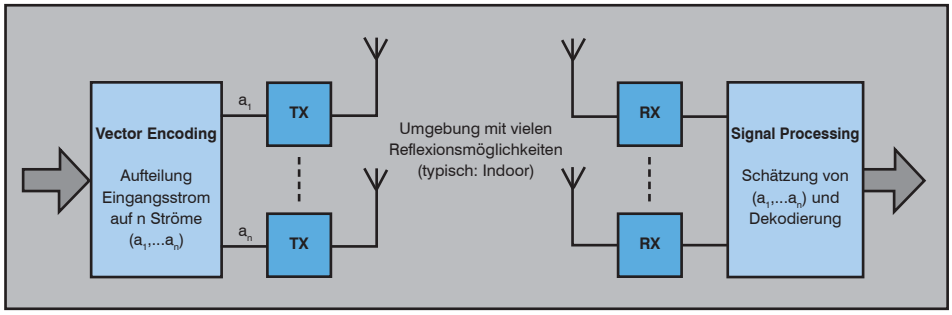


Abbildung 3: Zum Prinzip von MIMO

MIMO kann bei 11n mit bis zu 4 Spatial Streams betrieben werden. In Kombination mit der doppelten Kanalbandbreite ergibt sich dann eine Bitrate von 600 Mbit/s. Käuflich erwerben lassen sich derzeit übrigens nur 11n-Komponenten, die zwei oder maximal 3 Spatial Streams unterstützen.