ComConsult Research

Der Netzwerk Insider

Mai 2012

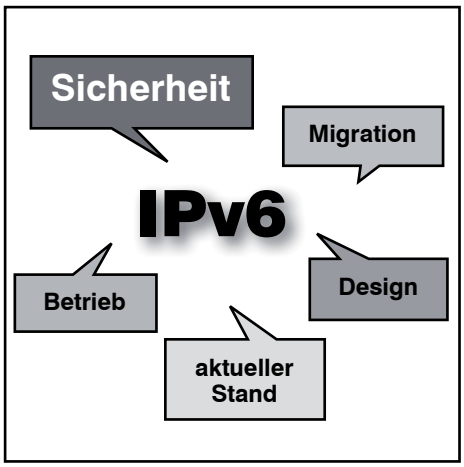
Systematische Weiterbildung für Netzwerk- und IT-Professionals

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-

Wireless-Versorgungs-Strukturen: kommen die Hybriden?

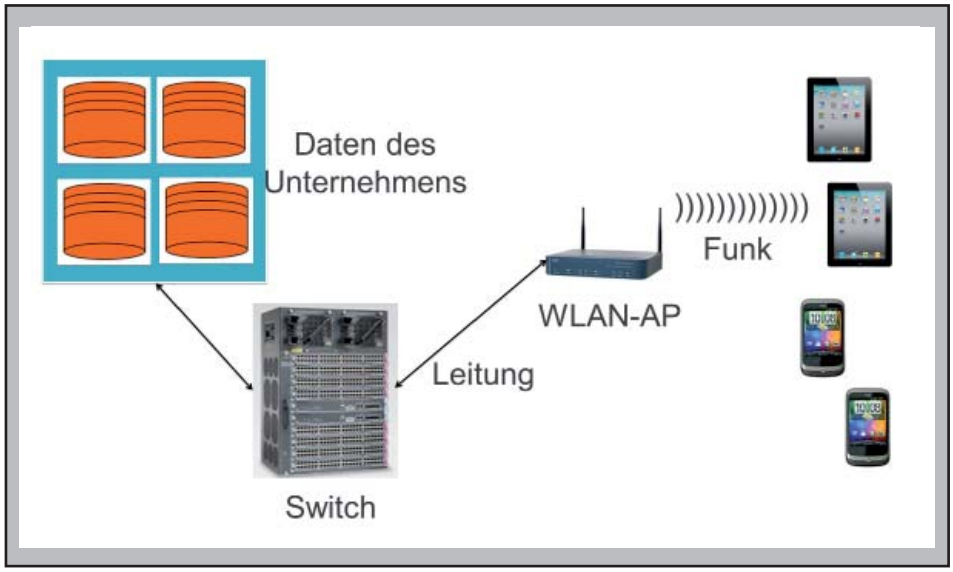


Abbildung 1: Versorgungsstruktur: WLAN

ter den WLAN-Zellen liegende Infrastruktur. Denn die gegenüber 11n/ac vier- bis fünffache Anzahl von Zellen zusammen mit der Notwendigkeit eines 10 GbE-Anschlusses für einen 5-7 Gbit/s.-fähigen AP führt zu erheblichen Kosten. Außerdem ist die Frage nach PoE für 10 GbE ungeklärt, meine persönliche Meinung ist, dass das aufgrund technischer Probleme nicht kommen wird. Betriebsaufwand und Kosten sind also der Preis für eine unternehmenseigene Lösung, der gegen das Gut der vollständigen Kontrolle über alle Daten und Wege, die sie nehmen, abzuwägen ist.

(Reine) LTE Infrastruktur

Jeder Controller in einem Unternehmen wird über die Frage nachzudenken haben, ob die Weiterentwicklung der eigenen WLAN-Infrastruktur angesichts der Verfügbarkeit von LTE wirtschaftlich überhaupt noch sinnvoll ist. Abbildung 2 zeigt, was dann entsteht: eine vollständig durch einen Provider abgedeckte Lösung. Hinsichtlich der Übertragungstechnik braucht man also nichts mehr zu machen, aber die spannende Frage ist jetzt, was mit den unternehmenseigenen Daten geschieht. Natürlich gibt es immer die Möglichkeit, Virtuelle Verbindungen aufzubauen. Hierfür bietet sich z.B. Carrier Ethernet vor allem mit den neuen, in Version 2.0 seit einigen Wochen festgelegten Möglichkeiten an. Ohne das weiter auszuführen, besteht der wesentliche Unterschied zwischen CE 1.0 und CE 2.0 in der Möglichkeit der Definition und Durchsetzung vollständig auch über kombinierte Domänen hinweg kontrollierbarer Service-Level.

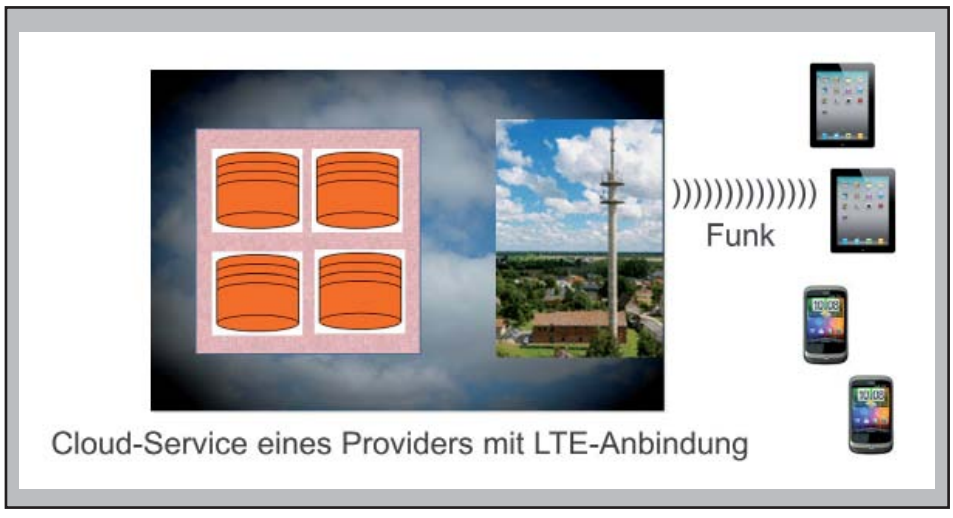


Abbildung 2: Versorgungsstruktur: LTE

Auch in Deutschland fallen die LTE-Preise bereits. Ende April 2012 bietet O2 den Einstieg für 14,90 pro Monat an. 7,2 Mbit/s. sind noch nicht die Welt, aber auch das wird sich schnell ändern. Etwas abstrus bei allen Anbietern ist das so genannte Datenvolumen. Ist das für einen Monat vereinbarte Volumen bei der Übertragung (z.B. 10 GB) aufgebraucht, wird die Datenrate heruntergestellt. Das ist schlicht eine Kinderkrankheit, die sich bei höherem Netzausbau verlieren wird.

Es ist aber blauäugig, anzunehmen, dass Provider es bei dem Anbieten bloßer Übertragungswege belassen. Vielmehr arbeiten sie ja schon heute daran, passende einfache und angereicherte Cloud-Services anzubieten. Die bekannte Telekom-Cloud sei hierfür ein Beispiel. Damit beeilen sie sich auch, um Boden auf dem Markt gut zu machen. Denn es gibt ja auch andere verlockende Angebote, wie z.B. G-Drive von Google oder iCloud von Apple, die alle neben dem einfachen Speichern auch Synchronisation und Zugriff über die Palette möglicher Endgeräte liefern. Provider haben allerdings den entscheidenden Vorteil, dass sie Cloud Service UND Zugriff aus einer Hand anbieten. Das ist ein Kampf, der im Massenmarkt schon einige Monate läuft, und sich mit weiter angereicherten Produkten in den Bereich der Unternehmensnetze fortpflanzt.

Also führen an dieser Stelle die Überlegungen zur Weiterentwicklung der Wireless Infrastruktur automatisch auf ein wesentlich gravierenderes Problemfeld, nämlich die Akzeptanz von Cloud-Lösungen. Das Dumme ist nur, dass hier die Entscheidungsprozesse wesentlich langsamer sind, weil es ja auch letztlich um existenzielle Fragen des Unternehmens geht.

Kommt man also vom Regen der teuren Weiterentwicklung eigener WLAN-Infrastrukturen nur in die Traufe der weitest gehenden Abhängigkeit von Providern?

Nein, denn es zeichnet sich glücklicherweise noch eine weitere Alternative ab.

Hybride Infrastruktur

Der Anstoß zu dieser Alternative kommt von Qualcomm. Bei der Präsentation des Gobi-Chips wurde die Möglichkeit erwähnt, diesen einfach mit einem WLAN-Controller Chip, wie z.B. den Atheros AR 6003 oder 6004 zu kombinieren und damit auf einfache Weise einen sehr preiswerten hybriden WLAN-AP herzustellen. Die Idee an sich ist nicht neu, schon vor Jahren hatte Intel vorgeschlagen, WiMax

Wireless-Versorgungs-Strukturen: kommen die Hybriden?

statt einer verkabelten Infrastruktur für die Versorgung der WLAN-APs zu verwenden. In der Breite ist das daran gescheitert, dass WiMax recht teuer und kaum verbreitet war und außerdem die Datenraten nicht zu denen von WLANs harmonierten.

Das ist aber jetzt fundamental anders. Der Gobi-Chip unterstützt Verbindungen bis zu 150 Mbit/s, also genau die Leistung besserer 11n Access Points. Qualcomm hat dabei natürlich vor allem an günstige Router für die Versorgung von Haushalten gedacht.

Grundsätzlich entsteht dabei die in der oberen Hälfte von Abbildung 3 zu sehende Infrastruktur: Endgeräte werden über WLAN angebunden, die hybriden APs über LTE. Das ist überall da praktisch, wo es sich nicht lohnt, ganze Straßenzüge für Glasfaserkabel aufzureißen. Die Konstruktion als solche ist auch skalierbar, mit Fortschritten im Leistungsangebot von LTE können dann eben auch mindestens 11ac APs angemessen versorgt werden.

Für Wireless-Infrastrukturen von Unternehmen ist das eine ganz spannende Alternative, denn nirgendwo steht, dass ein hybrider AP nicht auch eine normale Ethernet-Anbindung haben darf. Mit dieser kann er dann auch in die „normale“ Switching-Struktur des Unternehmens eingebunden werden. Das Unternehmen kann dann ja durchaus an den Stellen, wo es praktisch erscheint, das Cloud-Angebot eines Providers annehmen, behält aber auch eine eigene Infrastruktur. Das sehen wir in der unteren Hälfte von Abbildung 3.

Wenn schon durch die neue Klasse von Endgeräten erhebliche neue Anforderungen an die Unternehmen herangetragen werden, ist es doch sinnvoll, die neuen, multiplen Kommunikationsfähigkeiten dieser Geräte auch zu nutzen. Sie können heute schon alle 3G-Mobilfunk und 802.11n. Noch vor Ende des Jahres können sie auch 4G/LTE und wahrscheinlich auch 802.11ac. Neben den generellen Aspekten ergeben sich folgende klare Vorteile einer Hybrid-Lösung:

- Die Wireless Infrastruktur eines Unternehmens muss nicht wirklich vollständig mit WLAN-Technik realisiert werden. In Bereichen, wo es sich wegen z.B. einer geringen Nutzeranzahl oder geringen Kommunikationsaufkommens nicht lohnt, ein WLAN aufzubauen, kommunizieren die Geräte eben mit LTE

- Für Benutzer mit hoher Mobilität innerhalb des Unternehmens braucht man keine Klimmzüge hinsichtlich des Handovers zu machen, sie bekommen auch LTE

- Zwischen der Einbindung externer Mitarbeiter (z.B. Vertrieb) und interner Mitarbeiter braucht es keinen technologischen Bruch zu geben, weil über die Provider-LTE-Domäne einheitliche Sicherheits-Funktionen definiert werden können, die im Grundsatz auf der strikten Trennung zwischen Subscribern basieren

- Fällt das WLAN ganz oder teilweise aus, werden die betroffenen Benutzer über LTE umgeleitet. Eine Redundanz auf der Ebene der WLANs ist daher nicht zwingend erforderlich

- Weitere Redundanzmöglichkeiten ergeben sich gegebenenfalls durch die Kombination der unternehmenseigenen Daten-Infrastruktur mit der Cloud-Lösung eines Providers

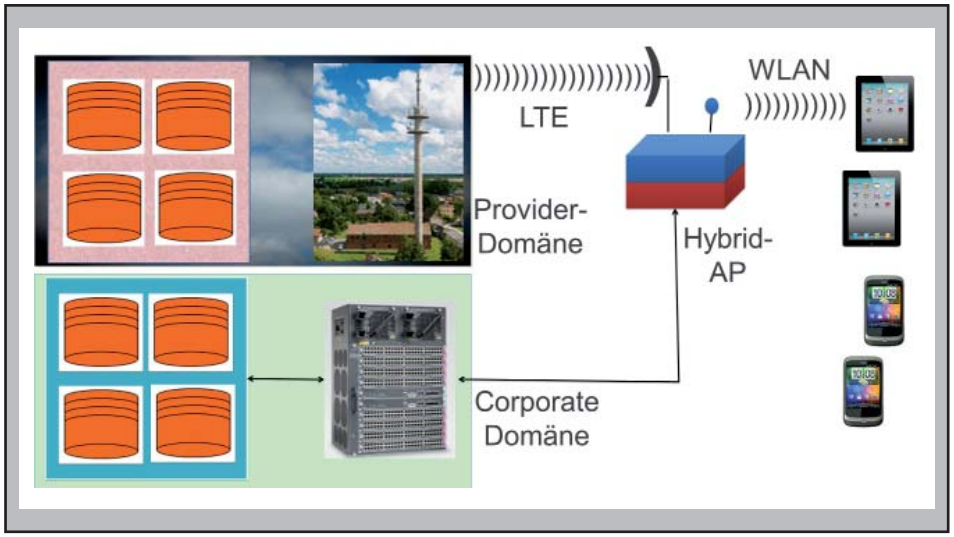


Abbildung 3: Versorgungsstruktur: hybrid

Abschließend sei noch erwähnt, dass auch die LTE-Standards eine Auffächerung eines leistungsfähigen Kanals ermöglichen, nämlich unter Benutzung der so genannte Femto-Zellen. Dies wird aber z. Zt. noch nicht wirklich ernsthaft verfolgt und durch Produkte hinterlegt.

Für den Privatbereich gibt es schon hybride LTE/WLAN-APs, die schlicht als LTE-Router bezeichnet werden und im Einkauf unter 100 Euro liegen. Vodafone, Deutsche Telekom und O2 verteilen alle den B390s-2 von Huawei. Eine professionelle Gestaltung sieht natürlich anders aus. So bietet z.B. Cisco LTE-Einschubkarten für die Integrated Services Router der Reihen 1900, 2900 und 3900 an. Diese Router liefern dann auch direkt Ethernet-Switching und PoE sowie umfangreiche Sicherheitsfunktionen einschließlich Firewalling, Filterung und Verschlüsselung in Hardware sowie WLAN-Controller und die einheitliche Steuerung größerer WLAN-Infrastrukturen. Die aktuellen LTE-Einschubkarten unterstützen 50/100 Mbit/s. für den individuellen Up/Downlink und insgesamt 350 Mbit/s. Die kompakten Geräte werden als „Branch Router“ angeboten und bieten neben praktisch allen denkbaren Schnittstellen zu kabelgebundenen WANs eben jetzt auch die Alternative LTE, was bei Cisco auch als WWAN (Wireless WAN) bezeichnet wird.

Fazit

Die durch die neuen Endgeräte an die Unternehmen herangetragenen Anforderungen an neue wireless Infrastrukturen sind umfangreich, aber die Lage ist nicht hoffnungslos. Auch in Deutschland werden die Provider ihre LTE-Angebote zügig ausweiten. Viele neue Endgeräte werden direkt in Bundles mit LTE-Verträgen auf den Markt drängen. Was dem Privatnutzer recht ist, kann dem Unternehmen nur billig sein. Durch hybride Access Points (oder eben um LTE angereicherte WLAN-Controller) werden zusätzliche Alternativen entstehen. Die Diskussion über neue wireless Infrastrukturen muss nicht notwendig in eine (wesentlich komplexere) Diskussion um die Auslagerung von Daten und Funktionen in Cloud-Dienste münden, sondern kann glücklicherweise davon weitest gehend getrennt werden, ohne dass man sich wichtige Optionen verstellen würde.

Ihr
Dr. Franz-Joachim Kauffels

Aktuelles Seminar

Sommerschule 2012 - Intensiv-Update auf den letzten Stand der Netzwerktechnik

Die ComConsult Akademie veranstaltet vom 25.06. - 29.06.12 in Aachen ihre "Sommerschule 2012".

Netzwerke unterliegen einer permanenten Weiterentwicklung. Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen. Die ComConsult Sommerschule 2012 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Top Experten der Branche gestalten das Programm dieser Intensiv-Schulung und bringen systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen in diesen Kurs ein. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

Die Sommerschule 2012 bringt Sie kompakt und intensiv in 5 Tagen auf den neuesten Stand der Technik in fünf ausgewählten, hoch aktuellen Themenbereichen und wendet sich an Teilnehmer mit Vorkenntnissen.

Frühbucherphase bis zum 31.05.2012

Wir bieten Ihnen exklusiv eine Frühbucherphase für die Sommerschule 2012 bis zum 31.05.2012 für eine rabattierte Teilnahmegebühr an.

Sommerschule 2012 zum Preis von € 2.290,--* netto

Die Buchung dieses Seminares innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Sommerschule 2012

Ich buche das Intensiv-Seminar
Sommerschule 2012
☐ vom 25.06. - 29.06.12 in Aachen
zum Preis € 2.290,-- netto*

*gültig bis zum 31.05.2012

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2012

18.06. - 19.06.12 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 18.06. bis 19.06.12 ihr "ComConsult IT-Sicherheits-Forum 2012" in Düsseldorf.

Im Moment zeichnen sich massive Veränderungen in der IT ab, zu denen die Informationssicherheit nicht nur eine Risikobewertung vornehmen, sondern sich selbst neu erfinden muss:

- Die Nutzung mobiler Endgeräte wie Smartphones und Tablets in Unternehmen und Behörden steigt exponentiell. Der traditionelle PC hat immer mehr ausgedient.
- Innovation in der IT findet im Consumer-Bereich statt und damit drängen Consumer-Techniken automatisch verstärkt in die Enterprise-IT.
- Mit Bring Your Own Device (BYOD) materialisiert sich der Wunsch private Endgeräte im Unternehmensnetz für Zugriff und Verarbeitung von dienstlichen Daten einzusetzen.
- Die Vision „IT als Dienst aus der Steckdose“, d.h. Unternehmensdaten und -anwendungen sind überall und mit jedem Endgerät verfügbar, wird immer ernster diskutiert.
- Die Zukunft der Kommunikation mit Clients ist drahtlos, d.h. WLAN, UMTS/LTE und Co. werden das klassische Kabel für die Client-Anbindung zur Nischenlösung machen.
- Unified Communications (UC) hat nicht nur die klassische TK aussterben lassen, UC verändert auch die IT. Traditionelle Zonenarchitekturen in RZ und Campusnetzen werden durch UC ad absurdum geführt.
- Consumerization dehnt sich auch auf den Anwendungsbereich aus. Bei sozialen Netzen, Skype und Co. geht es längst nicht mehr um die private Nutzung aus der dienstlichen IT heraus, sondern um die Nutzung für Unternehmenszwecke.
- Die eigene IT-Infrastruktur wird zunehmend durch externe Parteien betrieben, letztendlich ist Information das einzige Eigentum was noch übrig bleibt.
- Hosting von Rechenleistungen, Anwendungen und Speicher ist inzwischen so normal geworden, dass wir gar nicht gemerkt haben, dass Cloud Computing - anfänglich für den Enterprise-Bereich mehr belächelt als tatsächlich genutzt - die strategische Ausrichtung für IT-Dienstleistungen geworden ist.
- Das Data Center in a Box ist keine Vision mehr. Verschiedenste hochgradig dynamische komplett virtuelle IT-Infrastrukturen (d.h. Clients, Server, Netz und Storage), die gemeinsam auf einer physischen Hardware laufen, sind längst Realität.

Diese Entwicklungen in der IT haben direkte Konsequenzen für die Informationssicherheit:

- Die Integration von Smartphones und Tablets erfordert ein Mobile Device Management (MDM), das nicht monolithisch auf einen Systemtyp bzw. Hersteller ausgerichtet ist (z.B. Blackberry), sondern alle relevanten Systeme von iOS bis Android unterstützt.
- Für die IT-Sicherheit waren strikte Standardisierung und Kontrolle immer Kerninstrumente. IT-Sicherheit und Anarchie durch Consumerization der IT und BYOD kommen daher scheinbar einer Quadratur des Kreises gleich. Hier sind zunächst spezielle Techniken aus den Bereichen Mobile Device Management (MDM), Server-based Computing und Virtualisierung erforderlich, um private und dienstliche Daten zu trennen.
- Für BYOD sind außerdem spezifische Netzwerkkonzepte erforderlich, die letztendlich in eine Mandantenfähigkeit und die Notwendigkeit einer Netzzugangskontrolle (Network Access Control, NAC) münden.
- Mit BYOD gestattet man den Anschluss eines Fremdgeräts an die eigene Infrastruktur. Im WLAN ist dies mit vergleichsweise überschaubarem Aufwand verbunden. Möchte man ein solches Konzept auch auf das kabelbasierte LAN ausdehnen, wird man zur Trennung von Spreu von Weizen auch im kabelbasierten LAN oft um den Einsatz von IEEE 802.1X nicht herum kommen, was im Gegensatz zu WLAN im LAN ein höchstkomplexes Vorhaben ist.
- Mandantenfähigkeit erfordert stets die sichere Trennung der Informationen der Mandanten. Die traditionelle Methode der Informationssicherheit einer möglichst physikalischen Trennung auf Ebene des Netzes und der Endgeräte ist nicht mehr zeitgemäß. Virtualisierung und UC erfordern ein Umdenken in Richtung logischer Trennung und insbesondere in Richtung kryptographischer Techniken.
- Auf Zonenkonzepte auf Basis von Firewalls wird man trotzdem nicht verzichten können. Im Gegenteil: Zonenkonzepte in RZ und Campus werden zu einem normalen Gestaltungsinstrument. Schwerpunkte sind dabei die logische Trennung von Zonen in Virtualisierungsplattform, Netz und im Storage-Bereich.
- Die sichere Administration der Infrastruktur durch externe Dienstleister stellt besondere Ansprüche. Es sind Konzepte nötig, die zielgerichtet nur erlaubte Zugriffe gestatten und verhindern, dass ein Administrator ausgehend von dem administrierten System unberechtigt auf andere Systeme zugreift. Dies ist angesichts der Rechte eines Administrators technisch höchst anspruchsvoll und erfordert seinerseits spezifische Zonenkonzepte, in denen unter anderem Lösungen zur Entkopplung externer Zugriffe, zur Protokollierung von Administrationssitzungen und zur Nutzer- und Anwendungs-basierten Berechtigung von Zugriffen zum Einsatz kommen.
- Für den Nutzer einer virtuellen IT im Zeitalter des Cloud Computing muss sich die Informationssicherheit auf ihren Namen besinnen und Sicherheitsmaß-nahmen müssen sich auf die Informationen selbst konzentrieren. Kernelemente sind nicht nur die Zusicherung von Vertraulichkeit und Authentizität durch Verschlüsselungs-

techniken sondern immer mehr die Nachvollziehbarkeit von Änderungen an Daten (Revisionsfähigkeit) und die Kontrolle von unerwünschtem Abfluss von Daten, d.h. letztendlich Klassifikation von Daten in Verbindung mit Data Loss Prevention.

- Die klassischen Methoden und Prozesse der Informationssicherheit sind zu schwerfällig für eine IT, die maximale Mobilität für den Zugriff auf Information und für die Information selbst als Credo erhoben hat. Wir können nicht mehr für jede neue Anwendung aufwendige Sicherheitsbetrachtungen machen, wenn die Zeit zwischen Anforderungsanalyse und Produktivsetzung immer kürzer wird.

Aus diesen Gründen konzentriert sich das IT-Sicherheits-Forum 2012 auf folgende Themenbereiche:

- Sicherheit von Smartphones und Tablets, insbesondere iOS und Android
- Mobile Device Management (MDM): Techniken und Produkte
- Bring Your Own Device (BYOD): Techniken, Werkzeuge und Sicherheitskonzepte
- NAC mit IEEE 802.1X: Architekturen, Fallstricke und Projekterfahrungen
- Mandantenfähigkeit und Zonenkonzepte in RZ und Campus: Netz- und Firewall-Architekturen, Server- und SAN/NAS-Anbindung
- Sichere Netze: Risiken und Konzepte für UMTS/LTE und WLAN, Sorgenkind IPv6
- Sicherer Betrieb durch externe Dienstleister: Protokollierung und Berechtigung
- Cloud Computing: Sicherer Nutzung von Clouds, Aufbau sicherer private Clouds und Anforderungen an sichere Public Clouds
- Konzentration auf Information: Datenklassifikation, Data Loss Prevention und Revisionsfähigkeit
- Moderne Prozesse der Informationssicherheit: Integration in die schnellllebige IT

Wie auch in den Vorjahren greift das IT-Sicherheits-Forum 2012 die aktuellsten Entwicklungen im Bereich der Informationssicherheit auf. Das Forum ist wie folgt strukturiert:

- Vorträge mit Top-Referenten und Erfahrungsberichten aus der Praxis
- Neueste Forschungsergebnisse der ComConsult für zukunftssichere Investitionen
- Begleitende Ausstellung in Kombination mit einem Vortragswettbewerb zur Präsentation der besten Projekte und Ideen in der Veranstaltung
- Get Togehter am ersten Tag

Das ComConsult IT-Sicherheits-Forum 2012 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2012. Sie ist für jeden Entscheider, IT-Sicherheitsbeauftragten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult
IT-Sicherheits-Forum 2012

Ich buche den Kongress

ComConsult IT-Sicherheits-Forum 2012

☐ vom 18.06. - 19.06.12 in Düsseldorf
zum Preis von € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

im Hotel nikko Düsseldorf

_____ _____
Vorname Nachname

_____ _____
Firma Telefon/Fax

_____ _____
Straße PLZ,Ort

_____ _____
eMail Unterschrift

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Programmübersicht - ComConsult IT-Sicherheits-Forum 2012

Montag, den 18.06.2012

9:30 - 10:15 Uhr
Keynote: Das Ende der PC-Ära und die Konsequenzen für die Informationssicherheit
- Aussterben des klassischen Fat Client
- Schwindende Vertrauenswürdigkeit des Intranet
- Smart Phones, Tablets und Bring Your Own Device: Umgang mit unsicheren Endgeräten und Auswirkung auf Netz und Zonenarchitekturen
- Künftige Rolle von NAC und mandantenfähigen Campusnetzen
- Server-based Computing, Virtualisierung und Cloud Computing verändern die IT-Sicherheit
- Paradigmenwechsel: Maßnahmen auf Ebene der Daten selbst sind notwendig

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
Smartphones und Tablets: Risiken und Sicherheitsmaßnahmen
- Sicherheitsalptraum Smartphone & Tablet – Wie gefährlich sind mobile Endgeräte?
- Plattformen und Betriebssysteme im Vergleich – Ist Sicherheit à la Blackberry mit Android und iOS möglich?
- Bekannte Sicherheitslücken und Bedrohungen am Beispiel von Android und iOS
- Härtung mobiler Plattformen – Bordmittel und Zusatzprodukte

Dominik Zöller, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Mobile Device Management (MDM): Techniken und Produkte
- Von der Sicherheitsrichtlinie bis zur Inventarisierung - Was leistet Mobile Device Management?
- Von ActiveSync bis Afaria – MDM-Lösungen im Überblick
- Plattformabhängigkeit von MDM-Lösungen – Einschränkungen von Android und iOS
- Was muss MDM in Zeiten von BYOD leisten?

Dominik Zöller, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
Bring Your Own Device (BYOD) oder die Quadratur des Kreises
- Sicherer Zugriff auf Infrastruktur und Daten mit Sandboxing, Server-based Computing und Virtualisierung
- Reichen Sandboxing und Verschlüsselung für BYOD aus?
- Notwendigkeit von Mobile Device Management
- Server-based Computing und Smartphone-Virtualisierung
- Die Grenzen der Technik: Risiken von BYOD
- Nicht trivial: WLAN-Architekturen für BYOD
- BYOD im kabelbasierten LAN: Mission impossible?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Rechtliche Aspekte von BYOD und IT-Consumerization
- Grenzen der Kontrolle eigener Geräte des Benutzers
- Netzverantwortlichkeit des TK-Betreibers nach der TKG-Novelle 2012
- Beschäftigtendatenschutzgesetz - Neuregelung von Standortbestimmung und Stichprobenkontrolle
- Tunnelbau und rechtliche Grenzen der Maulwurfsbekämpfung
- Datensicherheit und Urheberrecht bei „gerooteten“oder „gejailbreakten“ Geräten

Ulrich Emmert, e/s/b Rechtsanwälte

15:00 - 15:45 Uhr
Network Access Control: Architekturen, Fallstricke und Projekterfahrungen
- Die Verschiebung von NAC als reine Security Lösung hin zur Netzwerkautomatisierung
- Multiple Mandanten, wie kommen die Nutzer ins richtige VPN?
- IEEE 802.1X und Co.: Welche Techniken zum Einsatz kommen, wo die Probleme liegen und wie in der Praxis damit umgegangen werden kann
- NAC als Basis für BYOD Projekte
- Die Anatomie eines typischen NAC Projektes
- Betrieb einer NAC-Lösung
- Projektbeispiele aus den Bereich Healthcare, Automotive, Government, Forschung im deutschsprachigen Raum

Markus Nispel, Enterasys Networks GmbH

15:45 - 16:15 Uhr Kaffeepause

16:15 - 16:45 Uhr
Einführung und Betrieb von IEEE 802.1X bei der IKB Data
- Herausforderung IEEE 802.1X für PCs,Thin Clients und Drucker
- Autorisierung mit ACLs
- Lessons learned: Typische Fehlersituation und wie damit umgegangen worden ist
- Standortübergreifende Einführung und Betrieb der NAC-Lösung

Alex Bruckhaus, Ulrich Wolf, IKB Data GmbH

16:45 - 17:30 Uhr
Ausstellerpräsentationen

ab 18:00 Uhr Get Together

Dienstag, den 19.06.2012

9:00 - 9:45 Uhr
Server-based Computing, Virtualisierung und Cloud Computing in der Analyse
- Kapselung von Daten und Anwendungen im RZ mit Server-based Computing und Desktop Virtualisierung
- Gefährdungen durch Zentralisierung von Clients
- Sind neue Konzepte beispielsweise für den Virenschutz erforderlich?
- Sicherheitsarchitekturen für Private Clouds
- Rolle von Public Clouds für die Enterprise IT
- Anforderungen an sichere Public Clouds

Dr. Behooz Moayeri, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr
Mandantenfähigkeit und Zonenkonzepte in RZ und Campus
- Mandantenfähige Campus-Netze: Techniken und deren Praxistauglichkeit
- Brauchen wir angesichts Server-based Computing und Cloud Computing noch Sicherheitsmaßnahmen im Intranet?
- Zonen- und Firewall-Architekturen im RZ
- Server-Anbindung und Load Balancing
- Zwiebelschalen-Modelle im Widerspruch zu Domänen-orientierten Zonenkonzepten à la Microsoft

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Web-Anwendungen, die Lösung aller Probleme?
- Die Architektur von Web-Anwendungen
- Neue Gefahren dank Apps
- Offline Web-Applikationen dank HTML5: ein Alptraum für die Datensicherheit?
- Server, Endgeräte, Smartphones und Tablets: wie sieht ein umfassendes Sicherheitskonzept aus?

Markus Schaub, ComConsult Research Ltd.

11:45 - 12:30 Uhr
Konzentration auf Information: Datenklassifikation, Data Loss Prevention und Next Generation Firewalls
- Next Generation Firewalls: Anwendungs - und User-zentrische Filterung der Kommunikation
- Methoden und Werkzeuge zur Klassifikation von Dokumenten und Daten
- Techniken zur Erkennung und Verhinderung eines Datenabflusses
- Data Loss Prevention: Host-basierte und Netz-basierte Systeme im Vergleich
- DRM und Co: Einsatz kryptographischer Mechanismen zur Kontrolle von Ausbreitung und Nutzung der Daten

N.N.

12:30 - 13:45 Uhr Mittagspause

13:45 - 14:30 Uhr
Sicherer Betrieb von Zonenarchitekturen
- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Infation droht
- SIEM: Sondermülldeponie oder sinnvolles Instrument des Security Incident Management?
- Kurzschluss in SAN und NAS vermeiden

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:30 - 15:15 Uhr
Nachvollziehbarkeit in derAdministration
- Typische Anforderungen und Herausforderungen
- Protokollierung von administrativen Zugriffen auf IT-Systeme
- Verfügbare Techniken und ihre Grenzen
- Marktüberblick und Auswahlkriterien

Marco Lorenz, cirosec GmbH

Ende der Veranstaltung 15:30 Uhr

Der Veranstalter behält sich Änderungen im Programm vor!

ComConsult-Study.tv

Sonderaktion im Mai bei ComConsult-Study.tv

Als besonderes Spezial diesen Monat bietet Ihnen ComConsult-Study.tv fünf Videos des Sicherheits-experten Dr. Simon Hoff zu einem Sonderpreis an.

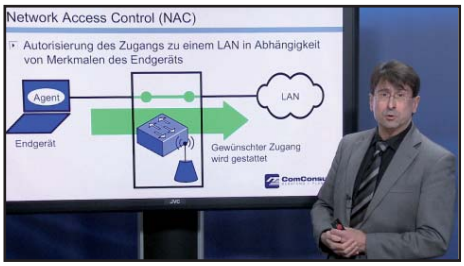
Bring Your Own Device
Referent: **Dr. Simon Hoff**
Zeit: 00:40:22
Einzelpreis: 59,00 € netto
Im Abo: kostenlos

Bring Your Own Device wirkt wie die Quadratur des Kreises: zufriedene Benutzer mit modernsten Applikationen bei gleichzeitig sinkenden IT-Kosten für das Unternehmen. Dr. Hoff analysiert in diesem hochaktuellen Video welche Rahmenbedingungen mit BYOD einher gehen. Die zentrale Frage ist: ist es möglich, Sicherheit für Unternehmens-Daten und Applikationen zu schaffen ohne die Privatnutzung des Benutzers einzuschränken?

Aufbau von Sicherheitszonen im RZ
Referent: **Dr. Simon Hoff**
Zeit: 00:32:44
Einzelpreis: 39,90 € netto
Im Abo: kostenlos

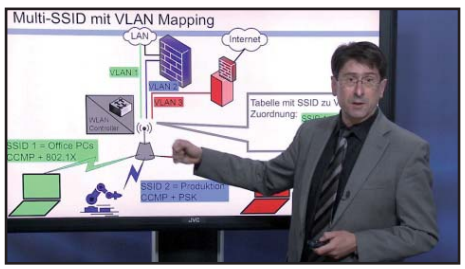
Jeder professionelle Angriff der Zukunft wird am Rechenzentrum ansetzen. Dies ist die unvermeidbare Folge der Zentralisierung von Daten, Applikationen, Servern und Clients. Dieses Video stellt alternative Lösungsansätze vor und diskutiert die damit verbundenen Probleme.

Grundlagen der Network Access Control
Referent: **Dr. Simon Hoff**
Zeit: 00:26:15
Einzelpreis: 39,90 € netto
Im Abo: kostenlos



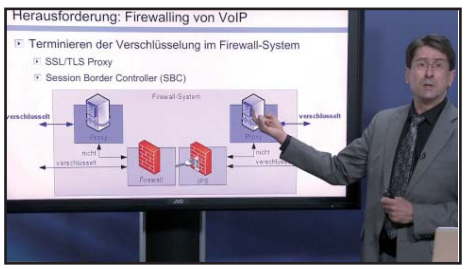
NAC: Steuerung des Zugangs von Endgeräten und Servern zu Netzwerken in Abhängigkeit ihrer Identifikation und Konfiguration.

Sicherheit in Wireless LAN
Referent: **Dr. Simon Hoff**
Zeit: 00:30:53
Einzelpreis: 39,90 € netto
Im Abo: kostenlos



Jede Funk-basierte Übertragung ist automatisch mit der Frage der Sicherheit der Übertragung verbunden. Dr. Hoff erläutert, warum das Thema brisant ist und stellt die verschiedenen Optionen zur Umsetzung von Sicherheit für verschiedene Typen von WLANs vor.

VoIP Sicherheit
Referent: **Dr. Simon Hoff**
Zeit: 00:34:44
Einzelpreis: 39,90 € netto
Im Abo: kostenlos



Dr. Hoff diskutiert mögliche und bekannte Bedrohungen für Voice over IP. Er stellt diesen typische Lösungs-Ansätze gegenüber, macht aber auch klar, dass einige dieser Ansätze komplex sein können.

Das Bundle dieser fünf Videos kostet nur € 149,90* netto. Sie sparen über 30%.

*Statt regulärer Preis € 218,60 netto.
Dieses Angebot gilt nur im Mai 2012.

Weitere Details finden Sie auf unserer Homepage unter www.comconsult-study.tv

Schwerpunktthema

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.

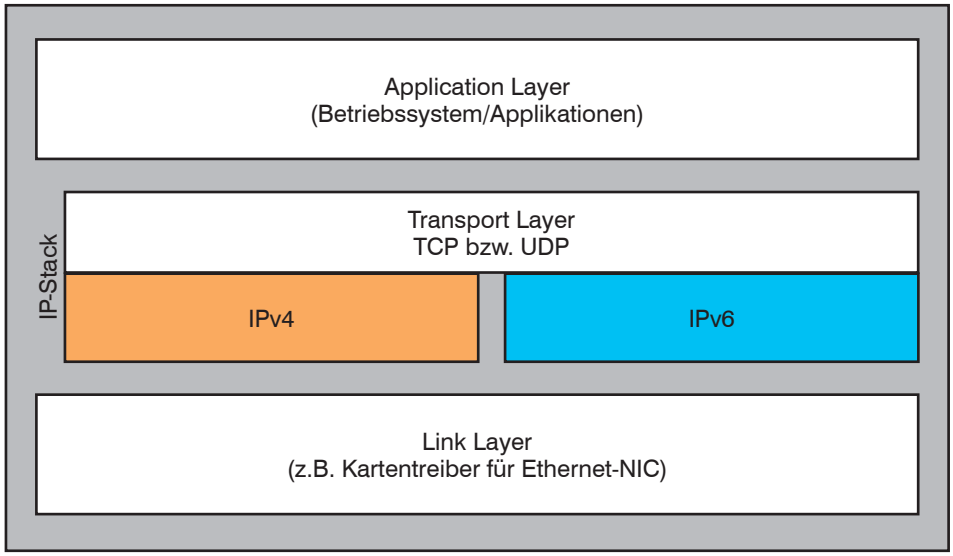


Abbildung 1: Dual-Layer-Ansatz

Ein nachträgliches Nachrüsten von IPv6 mit entsprechendem Roll-Out wird einem hier also erspart, wenn man jetzt eine aktuelle Windows-Version einführt, aber erst später IPv6 in die Fläche bringen wird. Dafür muss natürlich gestellt werden – und dies eventuell zweimal: zunächst vor Einführung von IPv6-Nutzung durch gezielte „Sperrung“, danach durch „sichere Konfiguration“ von IPv6.

Linux-Installationspakete umfassen typisch ebenfalls IPv6-Unterstützung. Wer hier nicht beim Installationsdurchlauf ausdrücklich auf das entsprechende Modul verzichtet (z.B. dies wegen bestimmter Anwendungen nicht ausschließen kann, damit diese installiert werden können), hat also einen prinzipiell IPv6-fähigen Rechner aufgesetzt.

Auch der Web-Browser und damit eine erste „Client-Anwendung“ ist IPv6-fähig: Der Browser „nutzt“, was ihm vom unterliegenden Betriebssystem geboten wird und was die über eine angegebene URL oder einen Link als Kommunikationsziel benannte Gegenseite an Kommunikation „versteht“.

2.1 IPv6 installieren und unkonfiguriert aktiviert lassen, aber vorerst nicht nutzen – ist das unbedenklich?

Mit der Funktionalität „Autokonfiguration“ verfügt eine IPv6-Implementierung über die Möglichkeit, sich zumindest Subnetzlokal funktionierende „Link Local“-Adressen („LLAs“) sofort und automatisch zu erzeugen. In Verbindung mit Mechanismen zum „Kennenlernen von Konfigurationsdetails mittels Befragen der Nachbarschaft“ (Stichwort „Neighbor Discovery“) muss man dann davon ausgehen, dass sich ein so mit einer LLA-Hilfsadresse ausgestattetes Gerät auch mit IPv6-Paketen im Netz meldet – und sich so als unter IPv6 angreifbarer Kandidat outet.

Man wird sich wundern, wie „geschwätzig“ ein solches Gerät selbständig sein kann, das lediglich mit einer LLA-Adresse („FE80:…“) ausgestattet ist:

(Der in Abbildung 2 erzeugte Mitschnitt entstand unmittelbar nach Aktivierung von IPv6 auf einer Windows 7-Installation, die als virtuelle Maschine realisiert und auf dem virtuellen Switch allein war, also nicht etwa von außen zu Kommunikation angeregt worden sein konnte. Mittels „Router Solicitation“ wird nach einem Subnetzrouter gesucht, der weitere Konfigurationsinformationen liefern soll, mit „DHCPv6-Solicit"-Paketen nach einem DHCPv6-Server …)

Außerdem – wer sagt denn, dass ein Angreifer wartet, bis ein mögliches Angriffsziel erstmals IPv6-Nutzkommunikation einleitet und dann erst versucht, anzugreifen? Eine andere Überlegung ist da leider viel wahrscheinlicher: IPv6-fähige Betriebssysteme halten Einzug, d.h. IPv4 und IPv6 sind nebeneinander vorhanden – vielleicht bietet sich ja unter IPv6 eine Schwachstelle, über die man das Gerät erfolgreich angreifen kann, um dann auch die IPv4-basierte Nutzung attackieren?! Wer z.B. erst einmal lauschenden Zugriff auf die Netzwerk-Schnittstelle eines Geräts ergaunert hat, kann jeden Verkehr über diese Schnittstelle „mitlesen“ und unbefugt weiter verwerten …

2.2 Gibt es denn schon Angriffsmethoden und -Werkzeuge für IPv6? Ja!

Na ja, aber erst einmal müssen ja Angriffsformen erarbeitet werden und entsprechende Angriffswerkzeuge zur Ver-

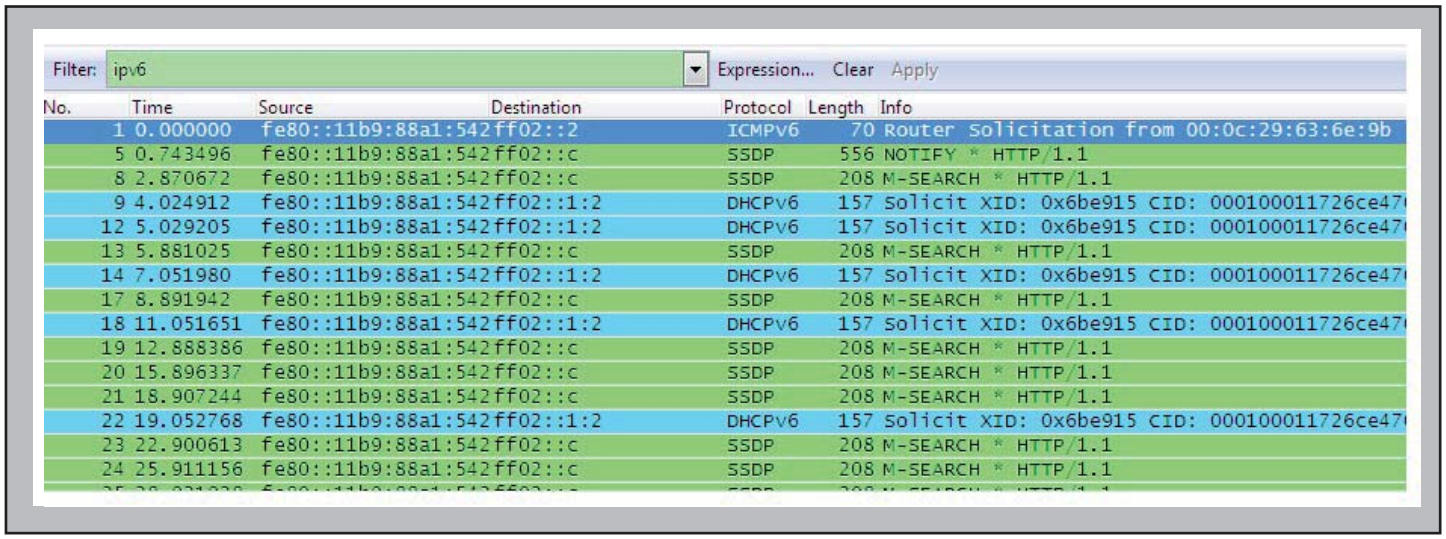


Abbildung 2: Aktivität eines Windows 7-Rechners nach Aktivierung von IPv6

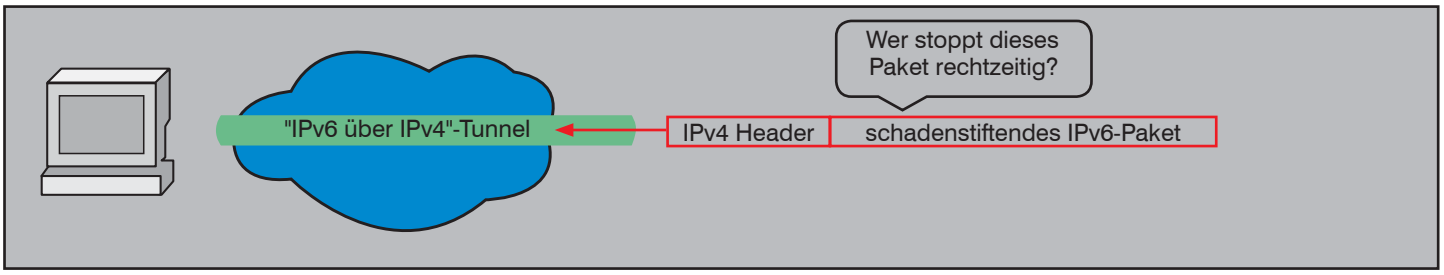


Abbildung 3: in IPv4 eingepacktes IPv6-Angriffspaket

fügung stehen. IPv6 ist in der Praxis noch so neu – das wird doch sicher noch etwas dauern? Oh nein! Es gibt längst etablierte Angriffsformen mit Blick auf IPv6.

Web-Präsenzen für Sicherheitsinteressierte wie „The Hacker's Choice" („THC", siehe www.thc.org) bieten bereits seit Längerem Werkzeuge an, mit denen man sich davon überzeugen kann, dass Angriffe auf IPv6 machbar sind, und mit deren Hilfe (mit der gebotenen Vorsicht wegen möglicher Systemstörungen und unter Beachtung des „Hacker-Paragrafen") man prüfen kann, ob die eigenen Systemkonfigurationen für solche Angriffe verwundbar sind. Das entsprechende veröffentlichte Tool-Paket für Penetrationstests von THC wurde zuletzt am 19.04.2012 aktualisiert und trägt die Versionsnummer 1.8 (ist also alles andere als „brandneu"), eine neue Version 2.0 ist für Ende des Jahres angekündigt.

Angriffe auf IPv6 und zugehörige Werkzeuge befassen sich dabei mit mehrerlei Ansätzen:

- Soweit Mechanismen und grundlegende Ansätze von IPv4 nach IPv6 übernommen wurden, können von IPv4 bekannte Angriffsformen unter IPv6 versucht werden.

- Neue Mechanismen unter IPv6 können evtl. für Angriffe missbraucht werden.

2.3 Migrationstechniken zur sanften IPv6-Einführung – auch hier lauern Gefahren

Angriffe auf IPv6 sind also realistisch, und wer noch keine „vertrauliche" Kommunikation über IPv6 betreibt, muss zumindest damit rechnen, dass als Vorbereitungsschritt über IPv6 angegriffen wird, um dann aus Innentäterposition die IPv4-basierten Lösungen ins Visier zu nehmen.

Basis dieser Vorgehensweise ist die parallele Aktivierung von IPv4 und IPv6 auf Geräten. In einer langen Übergangsphase der IPv6-Einführung wird dies eine zwingende Notwendigkeit sein: Eine Umstellung von IPv4 zu IPv6 nach Stichtagsprinzip ist unrealistisch, so unrealistisch sogar, dass dies in sehr großen Netzen schon allein für die Netzinfrastruktur eine echte Herausforderung darstellt. Entsprechend gibt es verschiedene Spezifikationen und zugehörige Implementierungen von Mechanismen, die es ermöglichen, IPv6-Pakete über eine IPv4-Netzwerkstrecke zu transportieren. Es handelt sich etwa um Tunneling-Techniken, bei denen die eigentliche IPv6-Kommunikation auf der „Tunnelstrecke" in IPv4-Kommunikation eingepackt wird.

Was als nützliche Hilfe bei einer sanften Migration zu IPv6 gedacht ist, eröffnet aber auch neue Möglichkeiten für Sicherheitsangriffe. Muss eine bislang erfolgreich gegen Angriffe von außen geschützte, IPv4-basierte Infrastruktur für Tunneling von IPv6 über IPv4 geöffnet werden, so kann ein Angreifer versuchen, den IPv6-Empfänger „durch den Tunnel" anzugreifen, um dann von diesem Empfänger aus weitere Angriffsschritte auf Ziele im internen Netz vorzunehmen. (siehe Abbildung 3)

Auch kann anders herum IPv6-Kommunikation über Tunnel-Mechanismen in einem eigentlich noch IPv4-basierten Netz derart Wege finden, dass ein IPv6-fähiger Rechner sich als solcher „verrät", ohne dass der Betreiber der Umgebung damit rechnet – und dann Angriffen auf IPv6-Basis durch den Tunnel ausgesetzt ist.

Man sieht:
Übergangstechniken zur IPv6-Einführung wie Tunneling müssen frühzeitig berücksichtigt und kontrolliert unterbunden bzw. eingesetzt werden.

2.4 Dual-Stack-Aktivierung von IPv4 und IPv6 ist gefährlich – gezielt vermeiden?

Voraussetzung für eine sanfte Migration zu IPv6, bei der schrittweise IPv6-basierte Kommunikation als Lösungsbasis Einzug hält, ist parallele Aktivierung von IPv4 und IPv6 auf beteiligten Geräten. So muss zum Beispiel ein Gerät, auf dem ein Tunnelende realisiert ist, (logischerweise) beide IP-Versionen unterstützen. Ein solches Dual-Stack-Gerät (Microsoft-Architektur: Dual-Layer-Gerät) ist aus Sicherheitssicht entsprechend „doppelt" gefährlich:

Zum einen kann, wie schon erwähnt, über die eine IP-Version das Gerät angegriffen werden, um dann die Umgebung von diesem Gerät aus unter der andern Version „von innen" zu attackieren. Zum anderen hat ein Angreifer gleich „zwei Chancen", eine IP-Verwundbarkeit zu finden, die einen erfolgreichen Angriff ermöglicht.

Sollte also eine gute IPv6-Sicherheitsleitlinie eine Vermeidung von Dual-Stack-Situationen als Vorgabe beinhalten?

Eine plausibel klingende Idee, jedoch zumindest in einer Frühphase der IPv6-Einführung wenig praktikabel. Bis alle Anwendungen und Dienste unter IPv6 nutzbar sein werden, können noch Jahre vergehen. Bis dahin muss ein IPv6-Einstieg aber längst erfolgt sein. Will man nicht mehr als nötig Migrationstechniken einsetzen und sich den damit verbundenen Betriebs- und Sicherheitsproblemen stellen müssen, so bleibt nur eine breit gestreute Dual-Stack-Nutzung als vorläufiger Ausweg. (siehe Abbildung 4)

Insgesamt bedeutet dies:
In einer Übergangsphase der schrittweisen Einführung von IPv6 addieren sich die Verwundbarkeiten von IPv4 und IPv6, und Migrationstechniken für Konnektivität von IPv4 und IPv6 erhöhen das Risiko zusätzlich.

3. Private IPv6-Adressen als „Sicherheitsmaßnahme für Jedermann"?

- Ein Beispiel für differenzierte Sicherheitsanalysen statt pauschaler Schnellschüsse -

Kann man bei der beschriebenen Ausgangslage zumindest die von IPv4 bekannten Methoden der Absicherung von Umgebungen in eine IPv6-Sicherheitskonzeption hinüberretten?

Dies geht zum Teil, zum Teil jedoch steht eine solche Vorgehensweise in starkem Konflikt zum gleichsam wichtigen Aspekt Betriebsaufwand. Ein grundlegendes Beispiel ist die Wahl des Adresstyps für „interne Kommunikation".

Gerät	Grund/ Zweck für dualen IPv4-/IPv6-Modus	wann
Router/ Layer 3-Switches/ Load Balancer	Unterstützung von IPv6-Kommunikation Ende-zu-Ende	vorbereitend vor IPv6-Einstieg
Layer 2-Switches	Einbindbarkeit in erste IPv6-basierte Management-Tools	spätestens zur Vorbereitung entsprechender Tool-Umstellung
Firewalls u.Ä.	Unterstützung gezielter Kontrolle von IPv6-Kommunikation	vorbereitend vor IPv6-Einstieg
Firewalls/ Netzkomponenten mit Nutzung als Paketfilter für IPv4	ggf. (produktabhängig) als Voraussetzung für gezielten Umgang mit IPv6-über-IPv4-Tunneln	vorbereitend auf IPv6-Einstieg / mit Einführung erster Dual-Stack-/ Dual-Layer-Clients
Router/ Layer-3-Switches/ Load Balancer	als Endpunkte für IPv6-über-IPv4-Tunnel	bei entsprechendem Tunnel-Bedarf (Empfehlung: möglichst Beschränkung auf Perimeter)
Firewalls	als Endpunkte für IPv6-über-IPv4-Tunnel	bei entsprechendem Tunnel-Bedarf (Empfehlung: möglichst Beschränkung auf Perimeter)
Endgeräte	Nutzung bei gemischter IPv4-/ IPv6-Landschaft bzgl. Diensten und Anwendungen	bei IPv6-Einstieg
DNS-Server u. ä. zentrale Infrastruktur-Server	IPv6-Bedienung für Umgebung in Migrationsphase mit paralleler Nutzung von IPv4 und IPv6	vorbereitend vor IPv6-Einstieg
Applikations-Server	sofern IPv6-basierte Anwendungsnutzung nur bei IPv4-Aktivierung möglich (produktabhängig!)	bei IPv6-Einstieg für derartige Anwendungen

Abbildung 4: Übersicht: (mögliche Gründe für) Dual-Stack-Betrieb auf verschiedenen Gerätetypen

Obwohl bei der Entscheidung zu 128 Bitlangen IPv6-Adressen das klare Ziel verfolgt wurde, ausreichend weltweit eindeutige („globale“) Adressen zur Verfügung zu haben, um jedes vernetzte Gerät der Zukunft Internet-fähig ausrüsten zu können, sieht auch IPv6 „private Adressen“ vor, die nur für die interne Kommunikation einer Umgebung genutzt werden können, im Internet jedoch nicht.

Solche Unique Local Addresses (ULAs) sind an einem eindeutigen Beginn der Netzwerkkennung erkennbar. Der Netzwerk-Präfix einer IPv6-ULA startet nach heutigen Festlegungen in der Hexadezimalschreibweise der Adresse mit „FC“ bzw. „FD“.

Eine mögliche Vorgabe in einer IPv6-Sicherheitsleitlinie zur Übernahme von Erfahrungen und Architekturen aus IPv4-Installationen könnte also lauten:

„Für rein interne Kommunikation verwende man Adressen vom Typ ULA. Diese werden von Routern am Rande des eigenen Netzes nicht nach außen übertragen, was vor Bekanntwerden interner Adressen und ungewollter direkter Kommunikation zwischen internen Rechnern und einem externen Angreifer schützt.“

Klingt verlockend, muss aber unter verschiedenen Aspekten genauer betrachtet und kritisch bewertet werden: Praktikabilität (Verfügbarkeit geeigneter Spezifikationen, Produktverfügbarkeit) und Betriebsaufwand (hier: Betrieb der Lösungen zur Umsetzung zwischen ULA-Adressen und extern verwendbaren globalen Adressen).

Die **differenzierte Abwägung zwischen „optimaler Prävention“ und Praktikabilität/Betriebsaufwand** soll an diesem Beispiel einmal genauer vorgeführt werden:

Vermeidung von Adressumstellungen bei nachträglichen Netzzusammenschlüssen

Für einen ULA-Präfix der Form „FD…“ kann auf freiwilliger Basis versucht werden zu verhindern, dass zwei Umgebungen denselben ULA-Präfix einführen (bei Interesse lese man etwa einmal unter http://www.sixxs.net/tools/grh/ula/ weiter). Dies ist aber eben eine freiwillige Vorgehensweise. Für „FC…“-ULAs wird möglicherweise zukünftig so etwas wie eine zentrale Verwaltung eingeführt (Eselsbrücke zum Merken: zentrale Verwaltung – Central Management – FCxx-Präfix). Dies ist aber Zukunftsmusik.

Na und?

Nun, ein bekanntes Phänomen in der IP-Praxis ist das nachträgliche Zusammenführen von ursprünglich separat aufgebauten internen Netzen, z.B. nach Firmenzusammenschlüssen. Sofern hier unabgestimmt Adressen mit gleicher Netzkennung (unter IPv4 typisch: 10.xxx) verwendet wurden, so ist ein Teil des Adressraums mit großer Wahrscheinlichkeit in beiden Umgebungen im Einsatz. Beim Zusammenschluss dieser Netze muss also entweder eine der beiden Umgebungen zur Vermeidung doppelter Adressen und damit Routing-Problemen adresstechnisch umgestellt werden, oder aber es wird unter IPv4 zwischen solchen „internen“ Teilnetzen ein NAPT-Übergang realisiert. Die hiermit bekannten Laufzeit- und Stabilitätserfahrungen unter IPv4 sind nicht unbedingt ermutigend, abgesehen von der Notwendigkeit zum Einsatz von NAT-Helper-Intelligenz auf solchen Gateway-Übergängen für alle Anwendungen und Dienste, die oberhalb des IP-Protokolls IP-Adressen als „Anwendungsdaten“ übertragen.

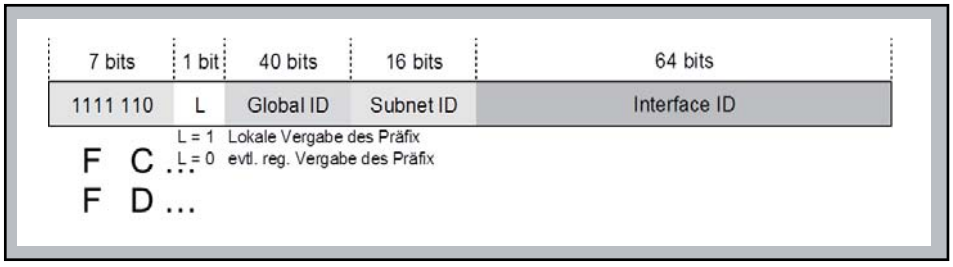


Abbildung 5: (Präfix zum) Adresstyp ULA

Na gut, man muss also darauf achten bzw. warten, dass zu IPv4-NAPT-Produkten eine IPv6-fähige Version verfügbar ist. Dann kann man aber doch unter Rückgriff auf die unter IPv4 gewonnenen Erfahrungen dazu übergehen, erfolgreich private IPv6-Adressen einzusetzen, um dann notfalls nachträglich unabgestimmt entstandene IPv6-Netze über NAPT-Gateways zu koppeln?

Leider nein:

Verfügbarkeit von NA(P)T für IPv6-Adressumsetzung?! Performance?
Derzeit gibt es keine IETF-Spezifikation bzgl. NA(P)T-artiger Umsetzung für IPv6-Adressen, eben weil man zunächst davon ausgegangen ist, dass für jedes Gerät, das mit externen Zielen kommunizieren soll, ja eine globale IPv6-Adresse bereit gestellt werden kann. Entsprechend philosophiert der aktuellste RFC zum Thema NAT und IPv6 (RFC 5902, Kategorie „Informational“) lediglich darüber, ob eine NAT-Spezifikation für Umsetzung zwischen IPv6-Adressräumen nicht doch sinnvoll sei, welche Ziele dafür sprächen, welche Fallen lauern, usw.

Eine verbindliche Basis für eine Hersteller-übergreifend einheitliche Implementierung einer Umsetzung zwischen IPv6-Adressräumen ist dies aber bei weitem nicht.

Konsequenzen:

- Es gibt keine herstellerunabhängige NAT-Spezifikation für IPv6 als Basis.

  Sofern hier eine Produktlösung angeboten wird, muss man sich selbst vergewissern, dass diese sich wie erwartet / gewünscht verhält. Ein Hersteller muss sich entsprechend erst einmal selbst Gedanken machen, wie er die Aufgabenstellung angeht.

- Im schlechtesten Fall muss für jede Form der Externkommunikation geprüft werden, ob es eine Application-Layer-Lösung zur Umsetzung gibt.

  Zu den Kandidaten, die bereits unter IPv4 eine solche Hilfe auf Anwendungsebene in Form einer „NAT-Helper“-Lösung benötigten, kommen jetzt auch die unter IPv4 pauschal über die NA(P)T-Basisfunktionalität abgewickelten Umsetzungen hinzu, für die unter IPv6 Proxy-artige Lösungen benötigt werden.
- Je komplexer ein Übergang wird, desto gefährlicher für die Antwortzeiten.

  Statt einer einheitlichen Umsetzungsbasis wie NA(P)T unter IPv4 droht bei IPv6 zur Umsetzung zwischen ULAs und globalen Adressen eine umfangreiche Sammlung an einzelnen Proxy- bzw. Helper-Funktionalitäten. Die entsprechende Software-Gesamtlösung wird leicht (noch) umfangreicher als bei IPv4-NAT-Gateways und stellt entsprechende Anforderungen an Hardware-Ausstattung und effiziente Programmierung, damit hier nicht ein so deutlicher Laufzeitverlust zu Buche schlägt, dass aus Anwendungssicht ärgerlich schlechte Antwortzeiten das Ergebnis sind.

  Selbst bei geeigneter Produktverfügbarkeit für die Umsetzung von ULAs auf globale IPv6-Adressen ist zumindest der Prüf- und Auswahlprozess bis zur erfolgreichen Produktauswahl aufwändiger als unter IPv4.

  Wenn es dumm läuft, müssen sogar für die insgesamt unterstützten Kommunikationsformen mehrere Produkte an einem Übergang zwischen ULAs und globalen Adressen kombiniert werden. Die Betriebskomplexität (Verträglichkeit, Change Management mit Blick auf Versionsführung und Patchen, …) kann hierdurch signifikant steigen, und auch die Verfolgung unter Sicherheitsgesichtspunkten (CERT-artige Begleitung des Produkteinsatzes) wird aufwändiger.

Provider-unabhängige Adressen besitzen und dennoch ULAs einsetzen?!
Zur Vermeidung von unter IPv4 kennengelernten negativen Effekten im Bereich Routing besteht eine wesentliche Strategie der Adressvergabe unter IPv6 in einer Provider-Bindung der Verwaltung von Netzwerkkennungen (IPv6-Präfix-Verwaltung) bzgl. globaler Adressen.

Am Ende der Vergabekette der Verwaltung von globalen Adressen, die diese weltweit eindeutig macht, stehen Provider oder Provider-artige „Netzbetreiber“ (das entsprechende Netzwerk ist nachgewiesenermaßen entsprechend groß, oder weist anbindungstechnisch die Eigenheit auf, „Multihomed“ zu sein). Diese erhalten relativ kurze Präfixe und vergeben aus dem entstehenden Adressraum Blöcke für Teilnetze, die sie „ans Internet“ anbinden.

Wer nicht die Eigenschaften aufweist, die zu einer Eigenverwaltung eines Adresspräfix berechtigen, erhält seinen Vorrat an globalen Adressen also von demjenigen Provider, der ihm den Zugang zu externen Netzen realisiert (providerabhängige Adressen, PA-Adressen). Dies bedeutet aber, dass zur Erhaltung „optimaler“ Routing-Tabellen der für dieExternkommunikation verwendete Präfix für globale Adressen zurückzugeben ist, wenn man den Provider wechselt. Betriebliche Folge: Ein Providerwechsel zieht hier eine Umstellung der genutzten globalen Adressen nach sich. Hiervor kann man sich bedingt durch interne Verwendung des Adresstyps ULA schützen – die interne Kommunikation ist von einem Providerwechsel dann nicht betroffen, da ja nur die globalen Adressen umgestellt werden müssen.

Allerdings: Wer sich einmal die Mühe gemacht hat, das Antragsverfahren für Provider-unabhängige (Provider-Independent-, PI-)Adressen zu durchlaufen und hiermit auch erfolgreich war, wird einen womöglich entstehenden hohen Aufwand zur Proxy-artigen Unterstützung verschiedenster Externkommunikation als Ersatz für einen bisherigen IPv4-NAT-Übergang doppelt kritisch sehen: Die damit verbundenen betrieb-

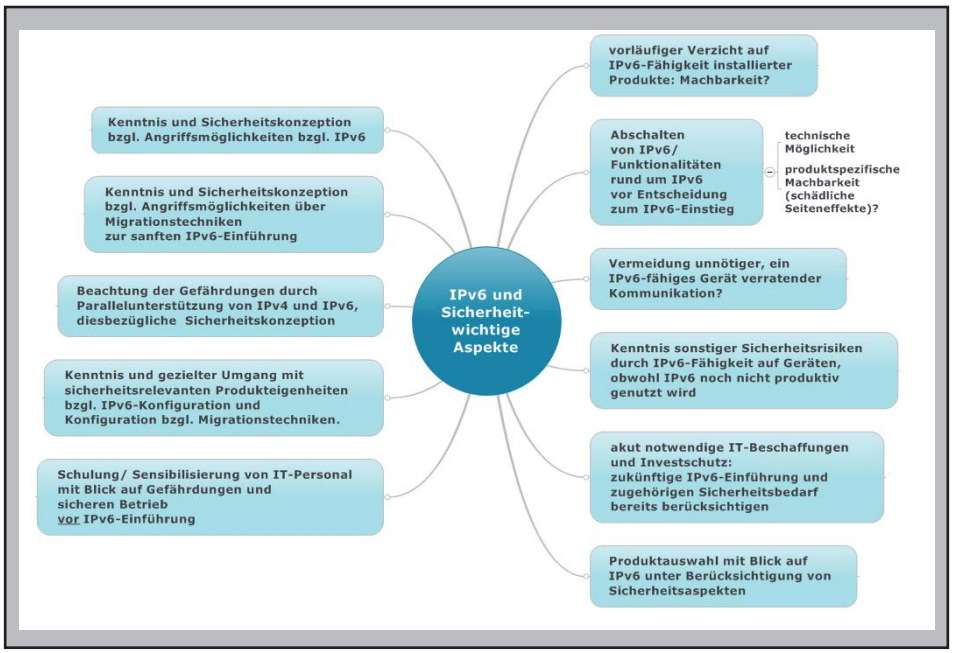


Abbildung 4: Übersicht: wichtige Elemente einer IPv6-Einführung unter Sicherheitsgesichtspunkten

lichen Unannehmlichkeiten bestehen, das Pro-ULA-Argument „Vermeidung einer Adressumstellung bei Providerwechsel“ ist für den Eigentümer von PI-Adressen nicht relevant.

Die diskutierten Aspekte führen nicht automatisch dazu, dass die Idee der Verwendung von ULAs als unsinnig einzustufen wäre. Allerdings ist es wichtig, bei der Entscheidungsfindung den entstehenden Betriebsaufwand zu berücksichtigen, ebenso die Notwendigkeit einer rechtzeitigen Verfügbarkeit entsprechender Produkte zur Adressumsetzung.

Für eine technisch orientierte Detailbetrachtung wird an dieser Stelle z.B. noch einmal auf RFC 5902 verwiesen. Sicherheitstechnisch sollte man aber insbesondere grundsätzlich bedenken: NA(P)T ist unter IPv4 nicht primär dazu erdacht worden, um eine Sicherheitsmaßnahme bereitzustellen, und ist auch bei IPv4-Sicherheitsarchitekturen keineswegs das tragende Element des Schutzwalls gegen Angriffe von außen.

Erst Sicherheitsgateways, die Paketfilterfunktion mit intelligenten Prüfungen auf Ebene der übertragenen Anwendungsdaten kombinieren, führen wirklich zur notwendigen Kontrolle über die Externkommunikation. NAT-Nebenwirkungen, die Angriffe erschweren, sind hier ein nettes „Add On“, nicht aber der Kern der Absicherung.

Es kommt unter IPv6 mehr denn je darauf an, ob der entstehende Planungs-, Produktauswahl- und Betriebsaufwand für einen Übergang zwischen internen und externen Adressen dieses Add On attraktiv genug bleiben lässt, um es „en passant“ als Element der Gefährdungsreduzierung mit zu nutzen. Die Verwendung des Adresstyps ULA als pauschal einzusetzendes Element einer „Sicherheitsleitlinie IPv6“ ist also ungeprüft gefährlich – hier muss man schon eine umgebungsspezifische Aufwand-Nutzen-Analyse vornehmen.

Dies ist typisch für die Auseinandersetzung mit IPv6 unter Sicherheitsgesichtspunkten: Einfache, stark präventive Ideen können gute Sicherheitsansätze für IPv6 sein, jedoch muss dies über eine Analyse verifiziert werden, welche den IT-Einsatz in einer Zielumgebung, die zugehörigen betrieblichen Rahmenbedingungen und die Produktsituation einbezieht.

Fazit: IPv6-Einführung unter Sicherheitsgesichtspunkten – wichtige Aspekte

Was haben die bisherigen Betrachtungen an Erkenntnissen gebracht?

Auch ohne bis hierher konkrete Fallbeispiele zu Sicherheitsangriffen auf IPv6 im Detail betrachtet zu haben, ergibt sich bereits jetzt das Bild einer komplexe Aufgabenstellung, wenn man das Thema IPv6(-Einführung) sicherheitstechnisch kontrolliert beherrschen will.

Diese Herausforderung muss man nun unter Berücksichtigung des IPv6-relevanten Verhaltens wichtiger Produkte annehmen, die Gefährdungslage konkretisieren und praktikable Ansätze für ein Sicherheitskonzept suchen – das ist sicherlich einen weiteren Insider-Artikel mit Beispielen wert …

Aktueller Kongress

Das Insider IPv6-Magazin passend zum ComConsult IPv6-Forum 2012

IPv6 kommt - IPv6 ist oft sogar schon da. Betriebsysteme wie Windows oder OSX haben von Hause aus einen aktiven IPv6 Stack. Microsoft schließt den Support sogar aus, wenn IPv6 deaktiviert wird. Abwarten und Aussitzen ist keine Lösung. Betreiber, Planer und Verantwortliche müssen sich somit mit dieser Technik auseinandersetzen.

In dieser Magazin-Ausgabe des Netzwerk-Insiders werden die Grundlagen des neuen Protokolles erklärt, ein Beispiel für den Betrieb von Direct Access vorgestellt und eine weitergehende Migrationstechnik behandelt.

Das Magazin startet mit einer zweiteiligen Übersicht über die neuen Funktionen von IPv6 von Petra Borowka-Gatzweiler: „IP Version 6 – das Internet der nächsten Generation“. Dieser erste Artikel einer 2-teiligen Serie behandelt folgende Fragen: Was passiert zur Zeit bei IPv6, wer nutzt es bereits? Welche Vorteile hat es? Wie sieht ein möglicher Aktionsplan aus? Wie sieht IPv6 technisch aus?

Danach folgt ein Artikel von Dietlind Hübner und Oliver Flüs, der den Einstieg in IPv6 am Beispiel der Adressplanung und

„Direct Access“ behandelt. Verschiedene Beiträge im Netzwer Insider haben bereits darauf hingewiesen, dass es an der Zeit sei, sich mit IPv6 so bald wie möglich zu beschäftigen, um nicht plötzlich überrollt zu werden. Wieso auf einmal die Eile, mag der eine fragen. Sollen das erst mal die anderen Kollegen im IT-Bereich machen, ich habe dieses Jahr genug anderes zu tun, mag der andere denken.

Der letzte Artikel von Markus Schaub beschäftigt sich mit der Frage, welche Rolle NAT bei der Migration spielen kann und was sich hinter der in Chrome genutzten Technik „Happy Eyeballs“ verbirgt. NAT bietet sich als logische Lösung für den Übergang zwischen reinen IPv4 Netzen und reinen IPv6 Netzen an. Allerdings ist diese Lösung nicht in allen Fällen trivial und die von IPv4 bekannten Mechanismen sind nicht 1:1 auf alle möglichen Übergänge zwischen Version 4 und 6 übertragbar. Hinzu kommt, dass es immer wieder Fälle gibt, in denen NAT versagt und andere Methoden zum Einsatz kommen müssen, um die Verbindung sicher zu stelle. Dieser Artikel beschäftigt sich mit den neuesten Entwicklungen in der Standardisierung, die eine „sanfte“ Migration auch unter widrigsten Umständen ermöglichen sollen.

Viel Spaß beim Lesen
Ihr Team von
ComConsult Research

Magazin-Download unter
www.comconsult-akademie.com/de/texte/artikel/ipv6-f%20magazin.pdf

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IPv6-Forum 2012

Ich buche den Kongress
ComConsult IPv6-Forum 2012
☐ vom 21.05. - 23.05.12 in Düsseldorf
zum Preis € 2.090,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 12

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht - ComConsult IPv6-Forum 2012

Montag, den 21.05.2012

Themenblock: Vision
9:30 bis 10:45 Uhr
IPv6-Vorbereitung: Warum, wann und wie?
- Warum kein Weg an IPv6 vorbei geht
- Welche Entscheidungen jetzt schon getroffen werden müssen
- Chancen und Risiken von IPv6
- Erfahrungen eines Umstellungs-Projektes

Markus Schaub, ComConsult Research Ltd.

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:30 Uhr
IPv6 Design & Infrastruktur
- Struktur und Umgang mit den neuen IPv6 Adressen
- Was sich bei Routing und VRRP geändert hat
- Einsatz von Infrastrukturdiensten: DNS und/oder DHCP
- Wie sieht ein modernes Netzdesign mit IPv6 aus?
  - Access-Bereich / Campus / Data Center / IPv6 und Layer-2 Konzepte wie VLANs, DCB, AVB
- Designvarianten I - Dual-Stack: Funktionsweise, Vorteile, Nachteile
- Designvarianten II – Tunneling: Funktionsweise, Vorteile, Nachteile
- Grundsätzliche Designvarianten III – Translation: Funktionsweise, Vorteile, Nachteile • Was müssen IPv6-fähige Layer-2- und Layer-3-Netzkomponenten können?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
IPv6@Bosch
- Warten oder starten - wann ist der richtige Zeitpunkt für ein Großunternehmen, mit IPv6 zu beginnen? Und warum?
- IPv6 betrifft die gesamte IT und alle Netzwerk-Funktionen - wo starten?
- Wie bindet man ein IPv6-Projekt erfolgreich in die Organisation ein?
- Welche Erfahrungen hat Bosch nach einem Jahr IPv6? Wo gab es Schwierigkeiten, was funktionierte auf Anhieb, was ist anders als bei IPv4?
- Ausblick: Wie geht es weiter mit IPv6 @ Bosch?

Anja Moog-Lölkes, Robert Bosch GmbH

14:45 bis 15:15 Uhr Kaffeepause

Themenblock: Sicherheit
15:15 bis 16:15 Uhr
Sicherheitsrisiken in IPv6
- Mehr Sicherheit durch IPv6?
- Der Reifezustand der IPv6 Implementationen
- Risiken automatischer Konfiguration
- Herausforderungen für den Firewall Einsatz
- Beschränkter Nutzen von Sicherheitsfunktionalitäten

Marc Heuse, Consultant

16:20 bis 17:20 Uhr
Sicherheit - IP Sicherheit: Neue Konzepte
- Welche Beiträge durch Netzkomponenten zur IPv6-Sicherheit absehbar sind, notwendige Sicherheitsbeiträge vernetzter Geräte („IPv6-Hosts“) im Zusammenspiel mit den Netzkomponenten
- Was sich im Bereich der Firewalls ändert
- Was man durch Auswahl aus Konfigurationsalternativen zur Sicherheit beisteuern kann
- Visionen vs. Produktverfügbarkeit - IPv6-Readiness bzgl. Sicherheit?

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr - Get Together

Dienstag, den 22.05.2012

Themenblock: Migration
9:00 bis 10:15 Uhr
Migrationstechniken
- Welche Phasen ein IPv6 Migrationsprojekt hat
- Wie die Entscheidung für ein Adresskonzept vorbereitet wird
- Wann das Netzwerk auf IPv6 migriert werden sollte
- Typische Einsatzszenarien während der Migration
- Wann Dual Stack zum Einsatz kommen sollte
- Wann Tunneling zum Einsatz kommen sollte
- Wann Translation zum Einsatz kommen sollte
- Überprüfung von IPv6 Readiness – Was bringt eine Zertifizierung?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

10:15 bis 10:45 Uhr Kaffeepause

10:45 bis 11:30 Uhr
IP Address Management für IPv6 - Welche Lösung passt ?
- Warum bei IPv6 eine zentrale Adressverwaltung unverzichtbar ist
- Welche Produkte es am Markt gibt
- Welchen Funktionsumfang alle Produkte gemeinsam haben
- Was die konzeptionellen Unterschiede der Lösungen sind
- Wie weit die IPv6- Integration in welchem Tool ist

Dipl.-Ing. Thomas Erhardt, n3k Informatik GmbH

11:35 bis 12:20 Uhr
Das Management erwartet für alle Fälle ein fertiges IPv6-Konzept, was nun?
- Worauf es bei der Bestandserfassung ankommt
- Was in der Zwischenzeit zu tun ist
- Wie mit nicht IPv6-fähigen Anwendungen umzugehen ist
- Was ab sofort zu beachten ist

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:20 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Anwendervortrag: Projektierung eines IPv6 Projektes

Themenblock: Aktueller Stand
14:50 bis 15:35 Uhr
Provider

15:35 bis 16:05 Uhr Kaffeepause

16:05 bis 16:50 Uhr
Software/VoIP

Mittwoch, den 23.05.2012

Themenblock: Betrieb
9:00 bis 9:45 Uhr
Cisco - IPv6 Strategie und innovative Migrations-Technik mit LISP
- IPv6 Strategie / IPv6 Zertifizierungen / IPv6 Roadmap
- Migration mit LISP

Gerd Pflüger, Cisco Systems GmbH

9:50 bis 10:50 Uhr
Betrieb - Einbindung von Endgeräten
- Der „Werkzeugkasten“ im Überblick - IPv6-Mechanismen mit Relevanz für den Endgerätebereich
- Der Endgerätebereich - betrieblich realistische Zielsetzungen in verschiedenen Phasen der IPv6-Einführung
- Dual Stack/ Dual Layer: ob, wann und wie lange zur Einbindung von Endgeräten? - bekannte Stolperfallen für den Endgerätebetrieb
- Theorie und Praxis - Konzeptideen und Produktunterstützung

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

10:50 bis 11:20 Uhr Kaffeepause

11:20 bis 12:30 Uhr
Mobilität, Smartphones & Tablets
- IPv6 für Anwendungen und zum Transport - zwei unterschiedliche Blickrichtungen
- IPv6 in Wireless LANs
- IPv6 in Mobilfunknetzen
- IPv6-Fähigkeit typischer mobiler Endgeräte
- Wann kommt die IPv6-fähige App?
- Ergebnisse unserer Praxistests

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Trouble-Shooting in IPv6-Umgebungen
- Protokoll-Know-how - Voraussetzung für erfolgreichen IPv6-Betrieb
- Protokollanalysatoren und IPv6
- Typische Fallstricke bei IPv6
- Beispiele aus der Fehlersuche-Praxis

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:50 bis 15:30 Uhr
Fazit & Ausblick
- Was waren die wichtigsten neuen Erkenntnisse aus den Vorträgen
- Welche Schlussfolgerungen können daraus gezogen werden
- Welche Handlungsweisen lassen sich daraus ableiten

Markus Schaub, ComConsult Research Ltd.

15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Neuer Report zum Subskriptionspreis

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

ComConsult Research veröffentlicht im Juni die Neuauflage des Reports „Cisco versus Microsoft: Wer hat die bessere Unified-Communications-Lösung?“.

Gelingt Microsoft mit seinem Einstieg in den Kommunikations-Markt die gleiche Erfolgsgeschichte wie seinerzeit Cisco? Schon mit der Veröffentlichung des Office Communications Servers hat Microsoft für Unruhe in diesem Markt gesorgt – ähnlich wie ihn der Einstieg von Cisco eine Dekade zuvor verursacht hat. Mittlerweile bietet Microsoft eine TK- und UC-Lösung an, die das Potential mit sich bringt, klassische TK-Anlagen abzulösen und im Markt einen sehr hohen Aufmerksamkeitswert hat. Konnte Microsoft seit dem Launch von Lync 2010 ihre Marktposition verbessern?

Der Eintritt beider Unternehmen in den Kommunikations-Markt zeigt einige Gemeinsamkeiten: In beiden Fällen hat ein auf seinem angestammten Gebiet marktbeherrschendes Unternehmen den Schritt in ein für es völlig neues Umfeld gewagt und dort mit der Unbekümmertheit eines Neulings und ohne Altlasten eine neue Sicht und neue Ideen in eine scheinbar ausgereifte Produktwelt eingebracht. Dabei könnten die beiden Kontrahenten kaum unterschiedlicher sein. Auf der einen Seite Cisco als Repräsentant der Datennetz-Welt und auf der anderen Seite Microsoft als der Software-Hersteller schlechthin.

Tatsächlich sind die Produktansätze beider Unternehmen zu Kommunikation und Kollaboration genauso unterschiedlich wie ihre Ausgangslage. Cisco hat mit dem CUCM eine moderne Voice- und Video-Architektur entwickelt und sich dann lange Zeit mit der Erweiterung auf umfassende Voice- und Video-Funktionalitäten aufgehalten. So ist der Erfolg von Cisco zwar unübersehbar, aber mittlerweile so groß, dass einige Berater, Analysten und Hersteller (so auch Microsoft) Cisco zu den „klassischen“ TK-Anbietern zählen.

Microsoft hat sich dagegen mit dem Thema "vollständiges Portfolio" gar nicht lange aufgehalten und mit Erfolg darauf gesetzt, dass die Mitbewerber Interesse daran haben werden, sich ihrerseits mit Microsoft-Produkten zu integrieren. Das gleiche gilt für das Thema Hardware: Microsoft hat von Anfang an Tischtelefone mit PC-Hardware, Tastaturen und Mäusen verglichen: Es werden sich schon genügend Hersteller finden, die so etwas bauen – vorausgesetzt der Markt ist groß genug. Microsoft trumpft mit ihrer Desktop-Dominanz, der Integration in die Office-Produktsuiten Outlook, Exchange, Sharepoint und Office sowie ihrer Erfahrung mit Server-Betriebssystemen. Cisco setzt dem eine durchgehende Produkt- und Protokollunterstützung im Netzwerk entgegen und trumpft mit einer äußerst umfassenden Portfoliolösung.

Hier setzt der aktuelle und kontroverse Report von ComConsult Research an. Er analysiert die bestehenden UC-Lösungen von Cisco und Microsoft auf dem Stand der neuesten Releases und stellt die spannende Frage, wer die bessere Lösung hat. Auch die erkennbaren Weiterentwicklungen werden dabei berücksichtigt. Der Report bewertet nicht nur die rein technische Funktionalität, sondern gibt auch Einschätzungen zum strategischen und wirtschaftlichen Einsatz und zur Zukunftssicherheit der Produkte ab.

Ausgehend von der Erklärung der technischen Rahmenbedingungen einer UC-Lösung sowie der Systemarchitekturen von Cisco und Microsoft werden die Produkte und Konzepte der beiden Hersteller auf der Basis eines ausführlichen Kriterienkatalogs miteinander verglichen.

Der Vergleich umfasst unter anderem die Bereiche:

- Architektur und Fehlertoleranz
- typische Einsatzszenarien
- Endgeräte
- Kontakte / Verzeichnisdienst, Presence
- Kommunikationsfunktionen: IM, Voice, Video, Konferenz, E-Mail-Integration
- Integration mobiler Benutzer
- Management und Administration
- Schnittstellen, Partner, Zertifizierung

Fax-Antwort an ComConsult 02408/955-399

Bestellung

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

☐ Ich bestelle den Report
Cisco versus Microsoft: Wer hat die bessere Unified-Communications-Lösung?
zum Subskriptions-Preis von € 348,--* netto
(*ab 01.06.12 regulärer Preis € 398,-- netto)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Standpunkt Troubleshooting

Das Schweizer Taschenmesser für den Netzbetrieb?

Der Standpunkt Troubleshooting von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Kennen Sie schon das aktuelle Top-Produkt eines bekannten Schweizer Herstellers? Ganze 80 Funktionen hat dieses Universalmesser. Aber mal Hand aufs Herz. Haben Sie schon mal versucht, damit im Garten einen Ast abzusägen oder am Auto eine Schraube festzudrehen? Ich benutze dafür lieber einen vernünftigen Fuchsschwanz oder nehme mir den passenden Schraubendreher aus einem gut sortierten Werkzeugkasten.

Auch Tools für den Netzbetrieb scheinen mir zuweilen diesem Schweizer Messer ähnlich. Oder sagen wir es anders: Der Anspruch an die Tools ist dem Anspruch an das Schweizer Messer vergleichbar: Man möchte ein Tool für alle Aufgaben. Selbstverständlich Multi-User- und Mandanten-fähig. Einerseits soll es das Front-End für den User Help Desk sein, das alarmiert und selbsttätig Tickets erstellt. Andererseits möchte der Netzwerk-Spezialist daraus detaillierteste Informationen für das Trouble Shooting zu Tage fördern können. Natürlich soll die Netzwerk-Dokumentation in graphischer Form hinterlegt sein und sich von selbst aktualisieren, wenn eine neue Komponente durch den Auto-Discovery-Prozess erkannt wurde. Alle Performance-Parameter im Netz sind über einen Zeitraum von mindestens einem Jahr vorzuhalten, schließlich weiß man ja vorher nicht, wer im Fall des Falles auf welche Parameter wann zurückgreifen muss. Und die Unternehmensleitung möchte jederzeit auf Knopfdruck einen Report über den Gesundheitszustand des Netzes erhalten. Und am Ende soll das Tool natürlich Kosten sparen. Mit anderen Worten, der hohe Investitionsaufwand soll sich durch Einsparungen auf der Personalseite am Ende amortisieren.

War ich deutlich genug? Es ist klar, dass es so etwas nicht geben kann. Ich nenne zwei Gründe: Erstens werden Sie so etwas kaum benötigen. Ich stelle mir nur gerade vor, mein Chef könnte sich auf Knopfdruck einen Report ziehen. Danke nein! Den Report möchte ich doch lieber selbst aufbereiten und meinem Chef

geben. Es kann schließlich sein, dass Erläuterungsbedarf besteht. Außerdem werden Sie wohl kaum alle verfügbaren Performance-Parameter im Netz aufzeichnen wollen, denn das schlägt sich bei manchem Tool in hohen Lizenzgebühren nieder. Als Beispiel führe ich gerne den Parameter „FCS Errors“ an. Tritt dieser Fehler auf, ist sofortiges Handeln vonnöten, um den Fehler abzustellen. „FCS Errors“ sind im Rahmen der Alarmierung zu behandeln.

Sie werden also zunächst Ihren Bedarf analysieren. Welche Informationen benötigen Planung, Betrieb und Trouble Shooting wirklich? Welche Informationen haben Ihnen in der Vergangenheit bei der Fehlersuche geholfen? In welchen Fällen hätten Sie eine Störung schneller beseitigen können, wenn Sie bestimmte Informationen gekannt hätten, die Ihnen aber mangels Tools vorenthalten waren. Wer in Ihrem Hause soll die Verantwortung für welches Tool übernehmen, und hätte auch Freude (!) daran? Welche Tools gibt es in Ihrem Hause bereits, welche werden nur mangelhaft genutzt? Wo könnten andere Betriebsprozesse auch ohne neue Tools die Kundenzufriedenheit erhöhen? Ich bin darauf bereits in meinen „Standpunkt“ vom Januar 2012 eingegangen.

Zweitens – und das erkennen Sie spätestens jetzt – werden Sie mit Tools keine Kosten sparen. Denn der personelle Aufwand für Einführung und Pflege ist in jeden Fall hoch. Häufig übersteigt er sogar die Anschaffungs- und Wartungskosten. In Anbetracht dessen empfehle ich, möglichst einfache und passgenaue Tools anzuschaffen. Suchen Sie gar nicht erst nach dem Schweizer Taschenmesser!

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

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 der-

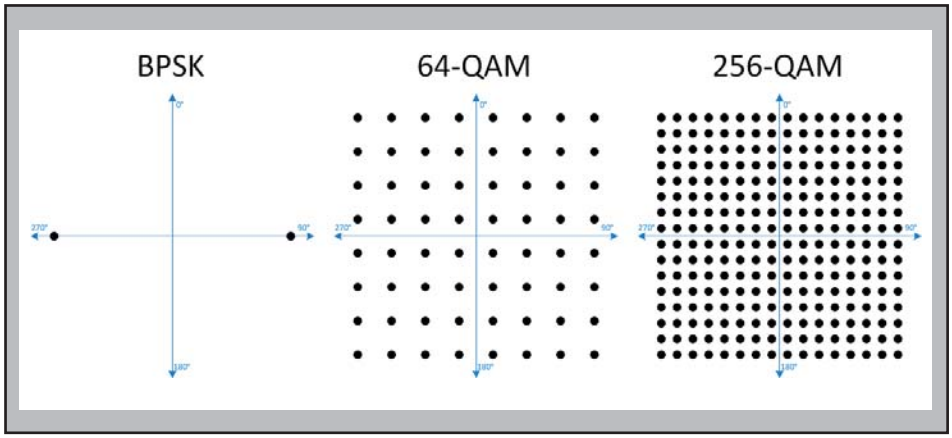


Abbildung 1: Gegenüberstellung einiger bei WLAN verwendeter Modulationsverfahren

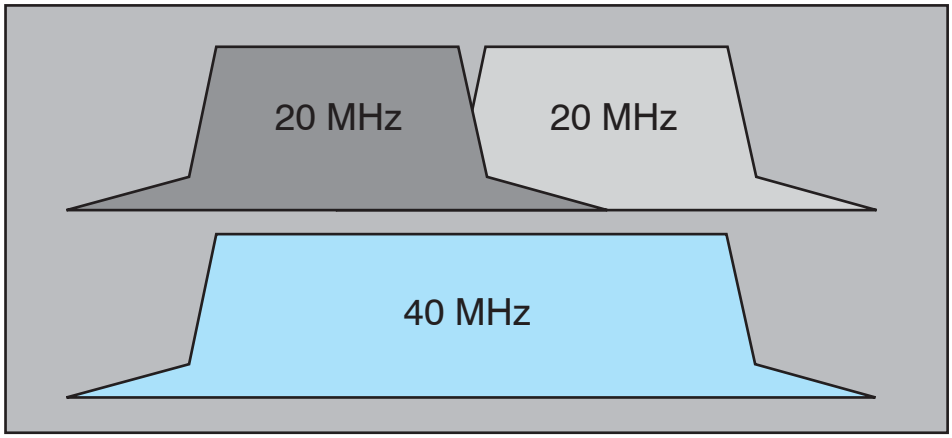


Abbildung 2: Verdoppelung der Kanalbandbreite

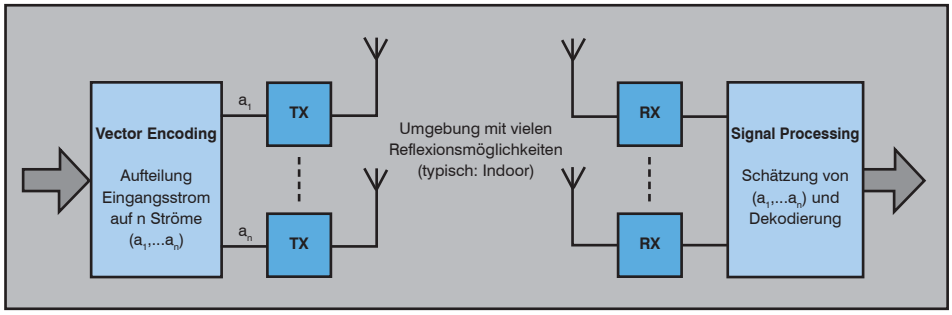


Abbildung 3: Zum Prinzip von MIMO

selben 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.

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.

Darüber hinaus soll noch eine weitere Technik nicht unerwähnt bleiben, die mit 11n eingeführt wurde. Wenn man nämlich mehrere Sender und Antennen zur Verfügung hat, kann man auf die Idee kommen, die Antennen mit demselben Signal anzusteuern, das jedoch für jede Antenne um einen individuellen Betrag phasenverschoben wurde. Diese Technik ist uralt, sie wurde unter anderem seit Ende der dreißiger Jahre für die Funknavigation eingesetzt (später als Consol-Funkfeuer bekannt). Ziel war es, durch Verändern der Phasenverschiebung die Richtwirkung der Antennengruppe zu beeinflussen, ohne diese mechanisch drehen zu müssen. Abbildung 4 versucht, die Wirkungsweise anschaulich darzustellen. Die vier phasenverschobenen Wellen ergeben eine Wellenfront, die gegenüber der Antennen-Ebene gedreht ist.

Und genau dieses Prinzip machen sich WLAN mit dem so genannten Beamforming zu Nutze. Der WLAN Access Point kann für jedes Datenpaket eine individuelle Senderichtung wählen, je nachdem, wo sich die Station gerade befindet. Die beste Antennenrichtung lernt er, indem er die zuvor von der Station empfangenen Signale und deren Phasenlage an den einzelnen Antennen auswertet und eine so genannte Steuer-Matrix berechnet. Access Point und Station tauschen Inhalte dieser Steuer-Matrizen aus; zu diesem Zweck stehen Felder in den Paket-Headern zur Verfügung.

Nach dieser langen Vorrede kommen wir nun endlich zum neuen „Very High Throuput“ (VHT) WLAN. Gegenüber 11n hat man eigentlich nicht viel Neues hinzuerfunden:

- Da ist zum einen das 8wertige Modulationsverfahren 256-QAM, das in Abbildung 1 bereits gezeigt ist. Sie erkennen, dass die Punkte nun sehr dicht beieinander liegen und erwarten, dass schon geringe Störungen die Übertragung beeinträchtigen werden. Immerhin lassen sich damit bereits 200 Mbit/s erreichen, mit Code-Rate 5/6 und ohne MIMO.

- Die Kanalbandbreite kann bei 11ac auf 80 MHz und sogar 160 MHz vergrößert werden. Das ergibt 433 respektive 866 Mbit/s. Alle möglichen Kombinationen aus Modulationsverfahren, Code-Rate und Kanalbandbreite sind in Abbildung 5 nachzulesen.

- MIMO wird nun mit bis zu 8 Spatial Streams unterstützt. Rechnerisch ergibt sich dadurch eine maximale Bitrate von knapp 7 Gbit/s – brutto wohlgemerkt.

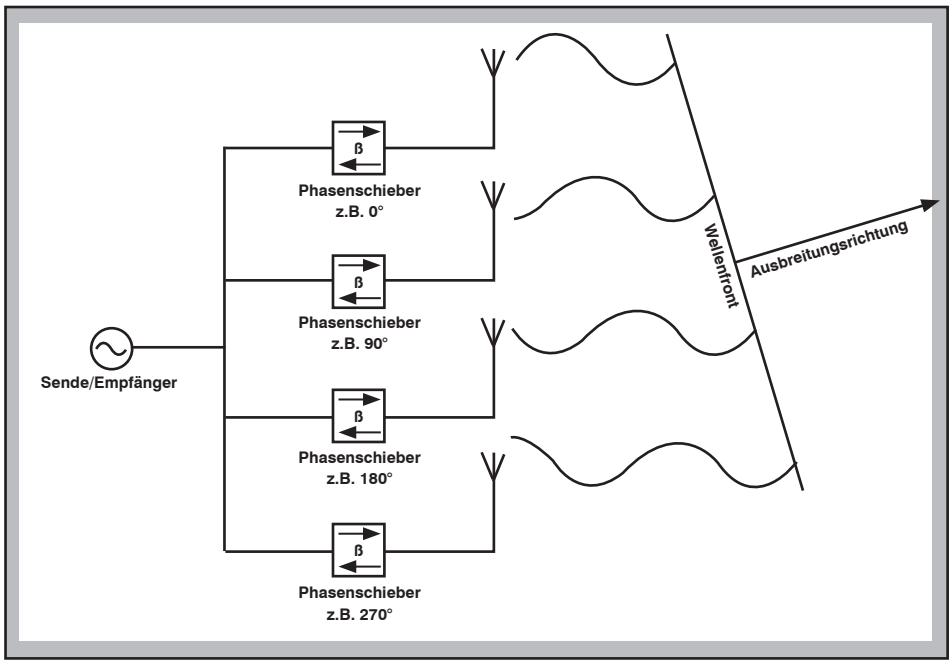


Abbildung 4: Zur Wirkungsweise des Beamforming

- Da man also nun bis zu 8 Antennen zur Verfügung hat, ist es auch möglich, mehrere Datenpakete gleichzeitig auszusenden, die an unterschiedliche Stationen gerichtet sind. Auch das grenzt an Zauberei. Multi User MIMO (MU-MIMO), wie dieses Verfahren genannt wird, teilt die bis zu 8 Spatial Streams auf mehrere Stationen auf. Ein Access Point kann also beispielweise zwei Stationen gleichzeitig ansprechen und dafür je 4 Spatial Streams einsetzen. Selbstverständlich lässt sich das mit dem entsprechenden Beamforming kombinieren; es werden also beispielsweise zweimal vier Spatial Strams in zwei verschiedene Richtungen ausgesandt. Beide Stationen teilen sich die insgesamt zur Verfügung stehende Bitrate.

Es lässt sich nachweisen, dass dieses Verfahren effizienter ist, als wenn man beide Stationen nacheinander mit der vollen Bitrate anspräche. Das liegt vor allem daran, dass man bei paralleler Aussendung nur einmal die Wartezeit zwischen den Paketen benötigt und dass die zur Empfänger-Synchronisation benötigte Präambel nur einmal ausgesandt werden muss. Allerdings steht nicht zu erwarten, dass MU-MIMO eine große praktische Relevanz bekommen wird. Der Grund ist einfach: MU-MIMO kann nur unter der Bedingung effektiv arbeiten, dass die parallel ausge-

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

Modulation	Code-Rate	Datenrate 20 MHz	Datenrate 40 MHz	Datenrate 80 MHz	Datenrate 160 MHz
BPSK	1/2	7,2	15,0	32,5	65,0
QPSK	1/2	14,4	30,0	65,0	130,0
QPSK	3/4	21,7	45,0	97,5	195,0
16-QAM	1/2	28,9	60,0	130,0	260,0
16-QAM	3/4	43,3	90,0	195,0	390,0
64-QAM	2/3	57,8	120,0	260,0	520,0
64-QAM	3/4	65,0	135,0	292,5	585,0
64-QAM	5/6	72,2	150,0	325,0	650,0
256-QAM	3/4	86,7	180,0	390,0	780,0
256-QAM	5/6	-	200,0	433,3	866,7

Abbildung 5: Erzielbare Brutto-Datenraten in Mbit/s bei IEEE 802.11ac mit einem Spatial Stream

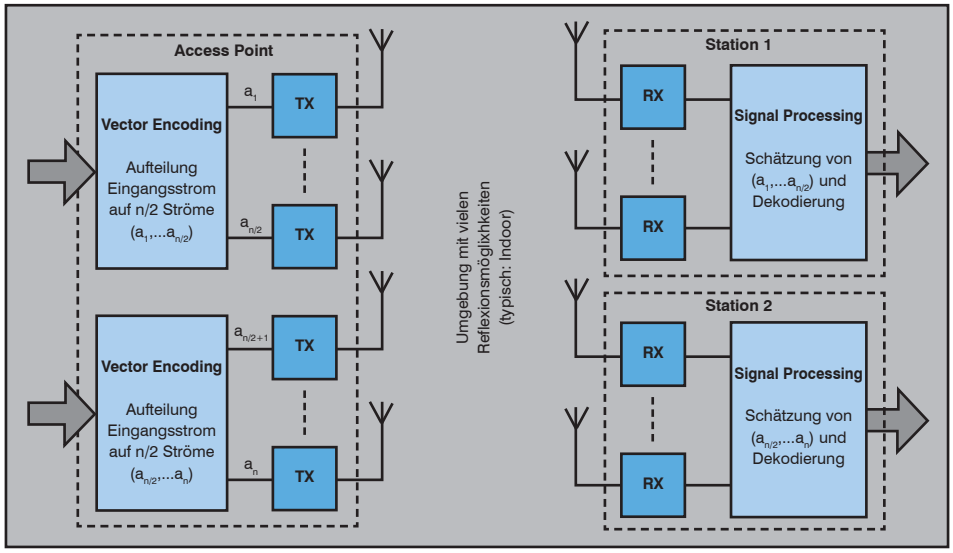


Abbildung 6: Zur Funktionsweise von Multi User MIMO (MU-MIMO)

sandten Pakete gleich lang sind. Und das wird sich in der Praxis wohl nur selten erreichen lassen.

Welche Leistung kann man nun vom 11ac-WLAN tatsächlich erwarten? Das wird zum einen davon abhängen, welche Chipsätze die Hersteller zukünftig anbieten werden. Heutige Chipsätze für 11n beherrschen in der Regel 2 oder 3 Spatial Streams. Man muss davon ausgehen, dass dies auch für die ersten 11ac-Chipsätze gilt. Erste Photos der in Las Vegas vorgestellten Prototypen von WLAN-Routern zeigen in der Tat drei Antennen. Offensichtlich hat man 80 MHz Kanalbandbreite realisiert und die 256-QAM. Mit 3 Spatial Streams ergibt das brutto 1,3 Gbit/s, was sich mit den Herstellerangaben deckt.

Zum anderen wird die erzielbare Bandbreite davon abhängen, welche Modulationsverfahren und Code-Raten in der Praxis tatsächlich eine störsichere Übertragung ermöglichen. Ein Hersteller hat auf der CES seine beiden WLAN-Router mit drei Antennenkabeln verbunden, um brauchbare Datenraten erzielen zu können. Es hieß, die hohe Dichte von Access Points auf der Messe könne eine schnelle Übertragung vereiteln.

Der Frage der Störanfälligkeit – oder besser – der Voraussetzungen für eine sichere Übertragung sollen die folgenden Überlegungen gewidmet sein. Sehen wir uns zu diesem Zweck, die Tabelle in Abbildung 7 an, die dem Draft 2 der IEEE 802.11ac entnommen ist. Hier wurden Mindest-Empfindlichkeiten definiert, die ein Adapter haben soll. Anders ausgedrückt, wenn die hier angegebene Leistung am Antenneneingang des Adapters anliegt, darf dieser bei der angegebenen Bitrate höchstens 10% Pakete verlieren. Zwei Beispiele:

- Mit 64-QAM, Code-Rate 5/6 und 20 MHz Kanalbandbreite (72 Mbit/s lt. Abbildung 5) liegt diese Grenze bei -64 dBm, entsprechend 0,4 Nanowatt
- Mit 256-QAM, Code-Rate 5/6 und 160 MHz Kanalbandbreite (867 Mbit/s lt. Abbildung 5) liegt diese Grenze bei -48 dBm, entsprechend 16 Nanowatt

Abbildung 5 zeigt die zu den Kombinationen passenden Übertragungsraten. Um also von 72 Mbit/s auf 867 Mbit/s zu kommen, muss die Leistung am Antenneneingang um 16 dB ansteigen, d.h. 40 mal so hoch sein. Sie werden feststellen, dass MIMO, also die Verwendung mehrerer Sender und Empfänger, in der Tabelle nicht berücksichtigt ist. Tatsächlich ist es so, dass sich beim Einsatz von MIMO bezüglich der Empfindlichkeiten der einzelnen Empfänger nichts ändert.

Modulation	Code-Rate	minimale Signalstärke 20 MHz	minimale Signalstärke 40 MHz	minimale Signalstärke 80 MHz	minimale Signalstärke 160 MHz
BPSK	1/2	-82	-79	-76	-73
QPSK	1/2	-79	-76	-73	-70
QPSK	3/4	-77	-74	-71	-68
16-QAM	1/2	-74	-71	-68	-65
16-QAM	3/4	-70	-67	-64	-61
64-QAM	2/3	-66	-63	-60	-57
64-QAM	3/4	-65	-62	-59	-56
64-QAM	5/6	-64	-61	-58	-55
256-QAM	3/4	-59	-56	-53	-50
256-QAM	5/6	-57	-54	-51	-48

Abbildung 7: Mindest-Signalstärken in dBm für eine Paketverlustrate < 10% laut IEEE 802.11ac Draft 2.0

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

Abbildung 8: Ausleuchtungsmessung, Grenze -72 dBm

Abbildung 9: Ausleuchtungsmessung, Grenze -56 dBm

Die Beispiele habe ich bewusst gewählt. Datenblätter für die neuen WLAN-Adapter liegen mir noch nicht vor, aber für gängige 11n-Adapter kenne ich die von den Herstellern angegebenen Grenzempfindlichkeiten. Sie liegen durchweg niedriger als hier angegeben. Für 72 Mbit/s benötigt ein WLAN-Adapter heute typischerweise nur -72 dBm Leistung am Antenneneingang. Man kann also vermuten, dass zukünftig ein typischer WLAN-Adapter für 11ac eine Leistung von -56 dBm benötigen wird, 16 dB mehr.

Wenn für hohe Übertragungsraten eine höhere Leistung benötigt wird, muss der Abstand zwischen Sender und Empfänger kleiner werden. Denn leider erlaubt die Regulierungsbehörde (in Deutschland die Bundesnetzagentur) nicht, dass man die Sendeleistung entsprechend erhöht. Dieser Zusammenhang lässt sich gut mit einem Messgerät für die WLAN-Planung zeigen, das die Ausleuchtung als farbige Karte darstellt.

Abbildung 8 zeigt eine solche Messung. Im Aachener Büro der ComConsult waren zwei Access Points aufgestellt worden. Anschließend haben wir den grün gezeigten Weg mit dem Messgerät abgeschritten. Das Gerät hat die tatsächlich gemessenen Signalstärken aufgezeichnet und im Grundriss farbig dargestellt. Die Darstellung wurde so parametriert, dass Werte kleiner -72 dBm als weiße Flächen angezeigt werden. Man erkennt, dass die beiden Access Points in der Lage sind, die gesamte Fläche mit ausreichender Signalstärke auszuleuchten.

Zum Vergleich haben wir in Abbildung 9 dieselbe Messung so parametriert, dass Werte kleiner -56 dBm als weiße Flächen angezeigt werden. Man erkennt sofort, dass die Ausleuchtung „löcherig“ wird. Es gibt also im Gebäude mehrere Bereiche, in denen wahrscheinlich eine Versorgung mit der bei 11ac höchstmöglichen Bitrate nicht möglich wäre.

Anschließend haben wir im Rahmen einer Simulation festzustellen versucht, wie viele Access Points benötigt würden, um auch bei der höchsten Bitrate eine Versorgung des Gebäudes sicherzustellen. Es zeigte sich, dass verglichen mit der heutigen Ausstattung etwa die doppelte Anzahl Access Points benötigt wird. Anders ausgedrückt: In diesem Gebäude müsste man in fast jedem Raum einen Access Point installieren, um von der vollen 11ac-Bitrate profitieren zu können.

Fällt ihnen etwas auf? Ganz am Anfang dieses Artikels habe ich geschrieben, dass WLAN im 60-GHz-Band (IEEE 802.11ad) die Grenzen eines Raumes nicht werden überschreiten können. Offensichtlich ist es bei IEEE 802.11ac im 5-GHz-Band nicht viel besser. Die Physik lässt sich also offensichtlich nicht überlisten: Gigabit-Bandbreiten erfordern eben einen Access Point pro Raum, so oder so.

Bleibt noch die Frage zu beantworten, wie denn zukünftig eine Zellplanung aussehen könnte, wenn die Zellen immer kleiner werden und dementsprechend dichter zusammenrücken. Wie Sie wissen, bietet ja nur das 5-GHz-Band ausreichend Platz für eine Kanalplanung mit mehr als 20 MHz Bandbreite. Denn das 2,4-GHz-Band ist ja eigentlich schon bei dieser Bandbreite zu schmal, bietet es doch nur drei überlappungsfreie Kanäle.

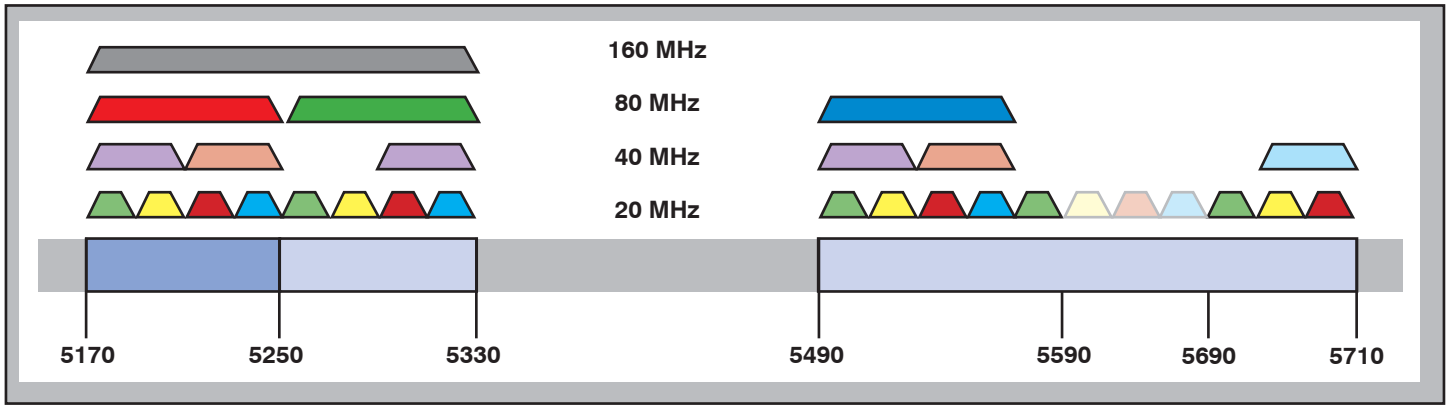


Abbildung 10: Kanäle im 5-GHz-Band

Im 5-GHz-Band gibt es derzeit 16 Kanäle mit 20 MHz Bandbreite. Sie erkennen das in Abbildung 10. „Derzeit" will sagen, dass in Europa durch eine Vorschrift der Norm ETSI EN 301 893 die Nutzbarkeit der drei Kanäle im Bereich von 5.600 bis 5.650 MHz stark eingeschränkt wird. Das hat dazu geführt, dass die Hersteller diesen Bereich in ihren Komponenten ausgenommen haben.

Verwendet man eine Kanalbandbreite von 40 MHz, lassen sich immer noch 6 Kanäle unterbringen. Bei 80 MHz sind es noch drei. Und wenn man eine Kanalbandbreite von 160 MHz einsetzt, kann man im ganzen 5-GHz-Band keine zwei Access Points nebeneinander betreiben, ohne dass sich ihre Signale überlappen.

Fassen wir also alles zusammen: Die Entwicklung der Wireless LAN schreitet unaufhaltsam fort. Motor ist, wie so oft, der Consumer-Bereich, weil sich hier schnell große Stückzahlen neuer Geräte bzw. Chips verkaufen lassen. WLAN gemäß IEEE 802.11ac sind eine Evolution des bereits eingeführten Standards IEEE 802.11n. Theoretisch werden sich mit WLAN auf Basis dieses neuen Standards Bitraten von bis zu 7 Gbit/s brutto erzielen lassen. In der Praxis der im Unternehmensbereich flächendeckend eingesetzten WLANs wird das aus zwei Gründen kaum möglich sein. Erstens ist wahrscheinlich die doppelte Anzahl von Access Points mit der entsprechenden Verkabelungsinfrastruktur vonnöten. Zweitens wird die Zellplanung auf Grund des erheblichen Bandbreitenbedarfs der neuen Technik vor eine unlösbare Aufgabe gestellt sein.

Wagen wir am Schluss eine Prognose: Die etablierte Technik der IEEE 802.11n mit 40 MHz Kanalbandbreite und einer resultierenden Brutto-Bitrate von bis zu 150 Mbit/s ist ein vernünftiger Kompromiss aus Übertragungsleistung einerseits sowie Störsicherheit bei der heute gegebenen Zellengröße andererseits. Mit demnächst 4 Spatial Streams sind dann die lange versprochenen 600 Mbit/s möglich. Ersetzt man nun die vorhandenen 11n Access Points durch neue mit 11ac, kommt man dank des neuen Modulationsverfahrens auf 800 Mbit/s, jedoch nur unter guten Empfangsbedingungen. Die mit diesen Komponenten ebenfalls bereitstehende höhere Kanalbandbreite wird sich in der Fläche kurzfristig nicht durchsetzen, da hierfür eine neue Zellplanung mit kleineren Zellen gefordert ist. Einzig die Weiterentwicklung der Chips in Richtung von MIMO mit 8 Spatial Streams wird deutlich höhere Bitraten in den vorhandenen Zellen ergeben, bis zu 1,6 Gbit/s.

Noch höhere Bitraten werden also mittelfristig nur punktuell zur Verfügung stehen. Und möglicherweise bietet hierfür die 60-GHz-Technik der IEEE 802.11ad die besseren Chancen – eine gänzlich neue Technik auf bisher ungenutzten Frequenzen, die also zu nichts kompatibel zu sein braucht. Denn bekanntlich ist ja Rückwärtskompatibilität ein Hemmschuh des Fortschritts.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Wireless LAN professionell, 14.05. - 16.05.12 in Nürnberg

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben.

Preis: € 1.890,-- netto

Storage: Planung moderner Speicher-Lösungen, 14.05. - 15.05.12 in Nürnberg

Dieses 2-tägige Seminar konzentriert sich auf Fragestellungen, die bei der Planung und dem Betrieb von Speicherumgebungen entstehen. In der Anforderungsanalyse werden die möglichen Einsatzszenarien wie etwa Datenbanken und virtuelle Umgebungen differenziert betrachtet. Zu diesen Anforderungen werden Lösungsansätze entwickelt, die sowohl heutige als auch zukünftige Technologien berücksichtigen. Die Kombination aus strategischen Überlegungen und technischen Maßnahmen bilden eine Leitlinie, welche Aspekte in welcher Form bei der Planung einer modernen Speicherinfrastruktur zu berücksichtigen sind.

Preis: € 1.590,-- netto

Service-Spezifizierung, 21.05. - 23.05.12 in Aachen

In diesem Seminar erlernen die TeilnehmerInnen die grundlegende Methodik der Service-Spezifizierung und die durchgängige Anwendung der Service-Spezifikation.

Preis: € 1.890,-- netto

Klassifizierung und Verfügbarkeits-Bewertung elektrischer Anlagen in Rechenzentren, 22.05. - 24.05.12 in Neuss

Der neue Lehrgang vom Sachverständigenbüro Dipl.-Ing. Karl-Heinz Otto erläutert die Grundlagen der in Arbeit befindlichen Richtlinie des BVS aus unabhängiger Sicht und 30 Jahren eigene Schadenerfahrungen und der Kollegen der öffentlich bestellten und vereidigten Sachverständigen der Bundesfachgruppe Elektronik und EDV.

Preis: € 1.890,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 04.06. - 06.06.12 in Köln

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance“-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam“ zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice“-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter“ Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Preis: € 1.890,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 11.06. - 15.06.12 in Aachen

Dieses 5-tägige Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt.Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können.

Preis: € 2.490,-- netto

Umfassende Absicherung von Voice over IP und Unified Communications, 11.06. - 12.06.12 in Köln

Dieses Seminar zeigt Wege auf, wie die Vorteile von Unified Communications für das Unternehmen nutzbar gemacht werden können ohne gleichzeitig die Sicherheit geschäftsentscheidender Kommunikation aufs Spiel zu setzen.

Preis: € 1.590,-- netto

WAN: Aktuelle Technologie und Erfahrungen aus Ausschreibungen, 11.06. - 12.06.12 in Köln

Das Programm des Seminars „WAN: Neue Verfahren und Erfahrungen aus Ausschreibungen“ bietet wertvolle Tipps und Empfehlungen sowohl zu technischen als auch zu organisatorischen Aspekten der Konzeption, der Planung, der Ausschreibung und des Betriebs von Wide Area Networks. Die Referenten des Seminars blicken auf langjährige Erfahrungen im WAN-Bereich zurück und vermitteln im Seminar Erkenntnisse aus Dutzenden von Projekten, in denen Wide Area Networks entworfen, ausgeschrieben und optimiert wurden. Der große Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen fließt ebenso in das Seminarprogramm ein wie die Expertise der Referenten bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb.

Preis: € 1.590,-- netto

Datenschutz- und steuerrechtliche Aspekte von Cloud Computing, 11.06. - 12.06.12 in Köln

Jederzeitige Verfügbarkeit der Daten und Kosteneinsparungen lassen Cloud Computing verlockend erscheinen. Wer jedoch Daten in fremde Hände geben will, muss sich über Datenschutz und Datensicherheit erhebliche Gedanken machen, da in Deutschland der Auftraggeber von IT-Dienstleistungen unabhängig von der vertraglichen Regelung die Haftung gegenüber Dritten in Bezug auf Datenverlust, unbefugter Nutzung oder sonstiger Datenschutzverletzungen übernehmen muss. Darüber hinaus gibt es zahlreiche Rechtsvorschriften, die die Speicherung in bestimmten Ländern oder den Datenzugriff aus diesen Ländern an bestimmte Voraussetzungen knüpfen oder sogar ganz verbieten.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
03.09. - 07.09.12 in Aachen
12.11. - 16.11.12 in Aachen

TCP/IP intensiv und kompakt
17.09. - 21.09.12 in Düsseldorf

Internetworking
11.06. - 15.06.12 in Aachen
22.10. - 26.10.12 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
12.06. - 15.06.12 in Aachen
23.10. - 26.10.12 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
26.06. - 30.06.12 in Aachen
04.12. - 07.12.12 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

Session Initiation Protocol Basis-Technologie der IP-Telefonie
18.06. - 20.06.12 in Bonn
29.10. - 31.10.12 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
11.06. - 12.06.12 in Köln
01.10. - 02.10.12 in Düsseldorf

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
24.09. - 26.09.12 in Bonn
26.11. - 28.11.12 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
10.09. - 11.09.12 in Berlin

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie