ComConsult Research

Der Netzwerk Insider

Dezember 2005

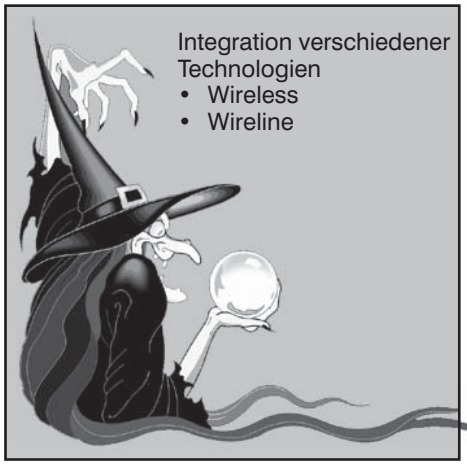
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends - Teil 1

von Dipl.-Inform. Petra Borowka

Die Trends zur Integration neuer Technologien und Dienste in vorhandene IP Netzwerke werden immer deutlicher. IP-Telefonie wird nicht mehr infrage gestellt, IP-Video steht vor der Tür, der Wireless Markt erlebte auch in 2005 ein weiteres Boom-Jahr. Anforderungen an konvergente Netze sowie die Integration von wireless und wireline bilden daher weiterhin einen Fokus für neue Entwicklungen. Der nachfolgende Beitrag befasst sich mit den neuen Technologien unter dem Blickwinkel der aktuellen Anforderungen.



Es bleibt spannend!

1. Erweiterte Anforderungen an Enterprise Netze und resultierende Änderungen

An „klassische“ Datennetzwerke werden zunehmend erweiterte Anforderungen gestellt, welche die bisher betriebenen Implementierungen oder Produkte noch nicht abdecken

- Mobilität
- Sprachdienste
- Stromversorgung über Ethernet
- Lokalisierung von Benutzern und Geräten
- Sicherheit
- Erweiterung der Management-Lösungen um Tools für Mobilität und Sprachdienste

weiter auf Seite 17

Zweitthema

Das Enhanced Wireless Consortium und seine Bedeutung für den Wireless Markt

von Dr. Franz-Joachim Kauffels

Vor wenigen Wochen hat sich das selbst so genannte Enhanced Wireless Consortium gegründet und für erheblichen Wirbel im Wireless Markt gesorgt. Es besteht aus dreißig teilweise sehr namhaften und bekannten Herstellern und hat die Beschleunigung der Implementierung von WLANs mit hohem Durchsatz zum Ziel. In diesem Artikel werden die wesentlichen Teilnehmer und Ziele vorgestellt sowie das Verhältnis zu IEEE 802.11n und die Bedeutung, die EWC einerseits für den WLAN-Markt an sich als auch speziell für die Unternehmensnetze in Europa hat, herausgearbeitet.

Die EWC-Mitglieder sind (Stand 25.10.2005) Airoha, Apple, Atheros, Azimuth, Broadcom, Buffalo, Cisco Systems, Conexant, D-Link, Gateway, Gemtec, Intel, Lenovo, Linksys, Lifepoint, Marvel, Metalink, Mitsubishi Electric, Netgear, nvida, Ralink, Realtec, Sony, Symbol, Toshiba, US-Robotics, Wild Packets, Winband und Zy-DAS.

weiter auf Seite 6

Top Veranstaltung

Netzwerk-Redesign Forum 2006

auf Seite 4

Zum Geleit

Netzwerk-Sicherheit: Hype oder Nutzen?

auf Seite 2

Report des Monats

Enterprise WLANs erfolgreich planen und betreiben

auf Seite 13

Zum Geleit

Netzwerk-Sicherheit: Hype oder Nutzen?

Die großen Hersteller von Netzwerk-Komponenten überschlagen sich mit immer neuen Konzepten und Produkten zur Netzwerk-Sicherheit. Auf den ersten Blick wirken diese Angebote durchaus überzeugend, doch auf den zweiten und intensiveren Blick offenbaren sich einige massive Mängel sowohl in den Produkten als auch in den Konzepten:

- Zum Teil werden isolierte Tools wild unter einem Marketing-Namen gemischt. Es gibt weder einen Zusammenhang in der Bediensystematik, noch ein gemeinsames Konfigurationstool, noch überhaupt ein passendes Rahmenkonzept. Das gemeinsame Element ist der Name, allerdings ist diese Vorgehensweise gerade bei Management-Tools nicht neu (siehe nahezu alle großen Management-Plattformen)

- In fast allen Produkten wird implizit unterstellt, dass sich der Bereich Client-Sicherheit dem Netzwerk unterzuordnen hat. Netzwerk-basierte Lösungen entscheiden, wann ein Client als sicher anzusehen ist. In der Praxis scheitert diese Sichtweise schon an der Zuständigkeit für den Client, die nun einmal nicht in der Netzwerk-Abteilung liegt

- Visualisierungskonzepte skalieren zum Teil nicht. In Präsentationen wird an einfachen und kleinen Umgebungen gezeigt, wie ein Angreifer versucht, auf einen Server zuzugreifen. Dabei ist die Erkennungsmethode so ausgelegt, dass in der Praxis im Zweifelsfall Hunderte von Flows darzustellen wären, was nun einmal nicht geht

Netzwerk-Sicherheit ist ohne Frage ein Fortschritt! Aber jeder akzeptable und sinnvolle Lösungsansatz setzt ein geeignetes Konzept voraus, das einige Bedingungen erfüllen muss:

- Das Konzept zur Netzwerk-Sicherheit muss ohne Brüche in ein Gesamtkonzept zur IT-Sicherheit einbindbar sein, die Schnittstellen zwischen den verschiedenen Systembereichen müssen klar definiert und in der täglichen Praxis handhabbar sein

- Der zu wählende Lösungsansatz muss auch organisatorisch ins Unternehmen passen, er darf keine Zuständigkeiten voraussetzen, die es in der Praxis in vielen Fällen nicht gibt. In Summe wird

ein Sicherheitskonzept nur funktionieren, wenn für ein Unternehmen auch eine geeignete organisatorische Lösung gefunden wurde. Dazu ist mindestens ein Abteilungs-übergreifendes Element, im Idealfall eine Stabsstelle Sicherheit mit Weisungsbefugnis erforderlich. Ohne den organisatorischen Gesamtzusammenhang entstehen in den Abteilungen Insellösungen, die zum einen nicht alle Gefahrenbereiche abdecken und die vor allem an den Schnittstellen nicht kompatibel zueinander sind

- Der gesamte Bereich der Netzwerk-Sicherheit sollte unter einer zentralen Oberfläche mit einem leicht zu handhabenden Bedienprinzip konfiguriert werden können. Die einzelnen Module dürfen nicht wild zusammengewürfelt sein

- Die Umsetzung eines Konzepts zur Netzwerk-Sicherheit darf nicht zu einer verstärkten Abhängigkeit vom Komponenten-Hersteller führen. Es darf dabei nicht übersehen werden, dass die Hersteller mit dem Thema Netzwerksicherheit für sich zwei Kernziele verfolgen. Zum einen sollen bestehende Netzwerk-Komponenten durch neue abgelöst werden, zum anderen soll dabei eine möglichst langfristige Bindung entstehen

Betrachtet man die aktuellen Trends im Bereich Netzwerk- und System-Management, dann drängt sich auf der Konzeptebene sofort ein zentraler Bereich auf:

- Alle sinnvollen und modernen Management-Ansätze, dazu zählt auch der Bereich Netzwerk-Sicherheit, basieren auf einer herstellerneutralen und zentralen Configuration Management Data Base CMDB. Dementsprechend gilt:

  - Eine zentrale Datenbank mit allen vorhandenen Endgeräten und deren Identitäten muss vorausgesetzt werden. Alle Zugangserlaubnisse für Geräte basieren auf Einträgen in dieser zentralen Datenbank. Es werden keine Individualschnittstellen zwischen Einzeltools aufgebaut, alles orientiert sich an der zentralen CMDB

  - Eine zentrale Benutzerverwaltung mit allen im Unternehmen vorhandenen Benutzern und deren Rechten muss unterstellt werden. Authentifizierungen erfolgen immer gegen diese zentrale Benutzerverwaltung oder eine damit synchronisierte Teilverwaltung

Weiterhin ist die zentrale Frage, ob folgende Annahmen getroffen werden können:

- Es gibt im Unternehmen ein Konzept zur Client-Sicherheit mit Virenschutz und Personal Firewall (letzteres zum Verhindern des Netzzugangs von nicht autorisierten Applikationen schon von der Client-Seite aus)

- Es gibt im Unternehmen ein Konzept zur Zugangssicherung auf zentrale Daten- und Applikations-Server

Können diese Annahmen getroffen werden, dann stellt sich die Frage, welcher Mehrwert durch Netzwerk-Sicherheit entsteht. Im Endeffekt kann man dies unterteilen in:

- Ein zulässiger und korrekt konfigurierter Client wurde durch einen Angriff übernommen und stellt nun selber eine Bedrohung dar. Er hat einen aktuellen Virenschutz und eine aktive Personal Firewall. Sollte der Angriff erfolgreich an der Personal Firewall (durch Nutzung einer zugelassenen Applikation) oder dem Mail-Virenschutz (durch keine geeignete Signatur im Virenscanner) vorbei kommen, dann stellt er natürlich eine Bedrohung dar. In der Praxis kann dieser Client nur durch ein abnormales Verhalten im Netzwerk identifiziert werden. Dies fällt dann in den Bereich Intrusion Detection/Prevention. Die damit verbundene Problematik der sichere-

ren Erkennung von Signaturen ist, denke ich, jedem bewusst. Hinzu kommt, dass ja bereits die lokalen Signaturen auf dem PC nicht ausreichten, um den Angriff zu erkennen. Dann stellt sich natürlich die Frage, warum die Netzwerk-Signaturen hier einen Mehrwert leisten sollen

- Ein zulässiger (sprich in der CMDB eingetragener Client), aber inkorrekt konfigurierter Client will auf das Netzwerk zugreifen. Dies ist kein Netzwerk-Thema. Wir müssen unterstellen, dass im Bereich der Client-Sicherheit eine Lösung geschaffen wurde, die für jeden definierten Client ein ausreichendes Maß an Sicherheit umsetzt. Es stellt sich die Kernfrage, ob Netzwerk-Sicherheit primär die Aufgabe hat, Versäumnisse im Bereich Client-Sicherheit zu beheben (darunter fallen auch organisatorische Versäumnisse)

- Ein unzulässiger Client will auf das Netzwerk zugreifen. Dies ist ein Thema für Netzwerk-Sicherheit, aber nur im Zusammenhang mit einer zentralen CMDB. Beim Zugriff auf den ersten Netzwerk-Switch muss bemerkt werden, dass der Client in der CMDB nicht eingetragen ist. Dieser Check kann sicher von einem erfahrenen Angreifer ohne große Probleme umgangen werden (durch Spoofen der Identität), doch werden auf diese Weise auf jeden Fall Gast-Clients und bisher nicht eingetragene Geräte erkannt. Erfahrungen mit großen Projekten haben gezeigt, dass dieser Ansatz gut funktioniert. Er setzt keinerlei herstellerspezifische Funktion voraus

- Ein unzulässiger Benutzer will auf das Netzwerk über einen zulässigen Client zugreifen. Ist der Client unzulässig, weil zum Beispiel ein Gast-Client, so kann nach der zuvor beschriebenen Regel sowieso kein Zugriff erfolgen. Dies ist sicher das Szenario, über das man nun unendlich diskutieren kann. Im Prinzip kann man sich auf den Standpunkt stellen, dass eine erfolgreiche Authentifizierung am Client im Zusammenhang mit einer Authentifizierung am Server bzw. an der Applikation ausreicht. In jedem Fall muss die Authentifizierung gegen ein zentrales Benutzer-Directory erfolgen. Auf der anderen Seite bietet speziell 802.1X genau die genormte Technologie, um diese Prüfung umzusetzen. Leider beinhaltet die Realisierung von 802.1X Wahlfreiheiten, die wieder zu herstellerspezifischen Lösungen führen können. Wie auch immer, der Bereich der Benutzer-Authentifizierung ist einer der Diskussions-Bereiche bei der Umsetzung von Netzwerk-Sicherheit.

An dieser Stelle soll nicht weiter ins Detail gegangen werden. Sinn der Aufstellung war der Nachweis, dass man ein Technologie- und Abteilungs-übergreifendes Konzept braucht. Und dies darf nicht am VLAN beginnen sondern muss Top-Down von der Bedarfslage runter gebrochen werden. Es kann auch nicht durch ein Produkt gekauft werden, Konzepte müssen immer Produkt-neutral sein.

Ich wiederhole die zentralen Statements:

- Jede Lösung zur Netzwerk-Sicherheit, die nicht auf einer zentralen CMDB zur Client-Verwaltung und einer zentralen Benutzer-Verwaltung aufsetzt, ist konzeptionell mehr als fragwürdig.

- Jede Lösung muss so aufgebaut sein, dass sie möglichst auf standardisierten und herstellerneutralen Funktionselementen aufbaut.

- Die Bedienung im Tagesbetrieb darf nicht durch eine Aufteilung auf mehrere Konsolen mit unterschiedlicher Bediensystematik zum täglichen Horror ausarten.

Naturgemäß sind diese Statements kontrovers. Gerne nehme ich Ihre Kommentare entgegen. Auf jeden Fall werden wir diesen Themenbereich auf dem Netzwerk-Redesign Forum Ende März 2006 intensiv diskutieren.

Ihr
Dr. Jürgen Suppan

Top-Kongress

Netzwerk-Redesign Forum 2006

Frühbucherphase bis zum 31.12.05

Die Comconsult Akademie veranstaltet vom 27. - 30. März das Netzwerk-Redesign Forum 2006.

Das Netzwerk-Redesign Forum, unser Top-Kongress des Jahres 2006, analysiert die aktuellsten Entwicklungen der Netzwerk-Technologien und bewertet Marktrends und Produktentwicklungen. Wir blicken für Sie hinter die Kulissen, geben Erfahrungsberichte aus aktuellen Projekten und bewerten die Praxis-Relevanz der neuesten Trends.

Im Mittelpunkt des Netzwerk-Redesign-Forums 2006 steht die Frage, wie das Design bestehender Netzwerke zur Erfüllung der immer weiter gehenden Kommunikations-Anforderungen verbessert werden kann.

Top-Analyse unseres Labors: neue Kommunikations-Anforderungen an Netzwerke
- Neue IT-Architekturen und ihre Anforderungen
- Globalisierung und Kommunikation
- Speicher-Technologien im Netzwerk
- Optimierter Client-Betrieb und die notwendigen Voraussetzungen
- IP-Telefonie, Konferenzschaltungen, Video/Multimedia/Dokument-Sharing
- RFID erweitert Netzwerk-Architekturen
- Logistik-Anwendungen im Netzwerk
- Produktions-Netzwerke und das Layer-2-Problem

Netzwerk-Redesign
- Bewertung eines bestehenden Netzwerk-Designs
- Design-Alternativen und ihre Nutzbarkeit
- Investitions-Sicherung
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Service-Level-Orientierung im Design
- Voice-ready-networks: Design-Grundsätze und Anforderungen aus der Praxis
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide, Enterasys, Extreme

Standardisierung und Technologie-Entwicklung:
- Was passiert hinter den Kulissen, was ist neu, wie relevant ist es?
- Welche neuen Standards sind verabschiedet, welche stehen vor der Tür?

- Was passiert in den Labors der Hersteller?

Optimierung des Netzwerk-Betriebs:
- Wie kann ein Netzwerk besser betrieben werden?
- Was leisten neue Werkzeuge?
- Service-Level-Operating im Tagesbetrieb

Hersteller und Produkte:
- Wie positionieren sich die Hersteller?
- Wie entwickeln sich wichtige Netzwerk-Produkte?
- Welche Vorteile können genutzt werden?
- Sicherheit und Netzwerke:
- Welchen Stellenwert haben Sicherheits-Lösungen im Netzwerk?
- Benutzeranmeldung im Netzwerk: welche Vorteile bietet das?
- Was leistet 802.1X, welche Projekterfahrungen existieren?
- Automatische Rechte- und Netzwerkzuordnung auf der Basis der Geräte- oder Benutzererkennung
- Was leistet eine Configuration Management Database CMDB? Generierung der Netzwerk-Konfiguration aus der CMDB?

IP-Telefonie erfolgreich einsetzen:
- Neueste Entwicklungen in der Analyse
- Stellenwert des SIP-Standards! Ausrichtung am Standard oder Konzentration auf einen Hersteller?
- Investitions-Sicherung: welche Alternativen der Migration zur IP-Telefonie bestehen?
- Wer hat die beste Lösung? Siemens versus CISCO versus Alcatel! Präsenz-Telefonie: ein neuer Standard oder eine Modeerscheinung?

Wireless LANs
- Neue Wireless-Standards: wo steht 802.11 im Vergleich mit 802.15/16/20
- Was bringt 802.11n?
- Wireless-Switching: wie reif ist die Technologie, was bringt sie
- Alternativen zum Wireless-Switching: Kontrolle großer Mengen an Access Points
- Aufbau einer Wireless-Hierarchie
- Redundanzkonzepte

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die Teilnehmer können dabei zwischen den Workshops wechseln.

Zurzeit sind folgende Intensiv-Trainings für den 4. Tag geplant:
- Konvergenz-Design: Integration von Voice und WLAN in LAN-Design
- Sicherheit im Netzwerk: neue Technologien sinnvoll einsetzen
- WLAN-Planung

Sie sehen, das Netzwerk Redesign Forum 2006 wird seinem Ruf als die führende deutsche Kongressveranstaltung zu Netzwerk-Technologien wieder voll gerecht. Wie in jedem Jahr so wird sich hier auch 2006 die Branche treffen. Die Mischung aus hersteller-neutralen Top-Referenten, den neuesten Technologie-Entwicklungen, hochaktuellen Projekterfahrungen und direkt umsetzbaren Empfehlungen aus der Praxis, einer hochaktuellen Ausstellung, der gleichzeitigen Anwesenheit vieler relevanter Hersteller hat diesen Kongress zum jährlichen Treffpunkt der Branche gemacht.

In den letzten Jahren war diese Veranstaltung immer ausgebucht. Als Mitglied des VIP-Verteilers haben Sie hiermit die einmalige Chance, sich bevorzugt einen Platz zu buchen bevor die öffentliche Werbung anläuft.

Netzwerk-Redesign Forum 2006

10% Frühbucherrabatt bis 31.12.05

Netzwerk-Redesign Forum 2005
27.03. - 30.03.06 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch im kommenden Jahr exklusiv eine Vorbuchungsphase für das Netzwerk-Redesign Forum 2006 bis zum 31.12.2005 für eine rabbattierte Teilnahmegebühr an. Wie im letzten Jahr besteht auch in diesem Jahr die Möglichkeit, die Veranstaltung 3-tägig oder 4-tägig (mit „Ein-Tages-Intensiv-Trainings“ am letzen Tag) zu buchen:

4 Tage Netzwerk-Redesign Forum 2006 mit „Ein-Tages-Intensiv-Trainings“
zum Preis bei Buchung bis 31.12.05 von € 1.990,-
statt regulär € 2.190,- zzg. MwSt.

3 Tage Netzwerk-Redesign Forum 2006 ohne „Ein-Tages-Intensiv-Trainings“
zum Preis bei Buchung bis 31.12.05 von € 1.590,-
statt regulär € 1.790,- zzg. MwSt.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeite Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2006

Ich buche den Kongress
Netzwerk-Redesign-Forum 2006
vom 27.03. - 30.03.06 in Königswinter

mit „Ein-Tages-Intensiv-Training“
☐ Konvergenz-Design: Integration von Voice und WLAN in LAN-Design
☐ Sicherheit im Netzwerk: neue Technologien sinnvoll einsetzen
☐ WLAN-Planung
zum Preis von € 1.990,- zzgl. MwSt.*

☐ ohne „Ein-Tages-Intensiv-Training“
zum Preis von € 1.590,- zzgl. MwSt.*
***Preise gültig bis 31.12.05**

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

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

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

Zweitthema

Das Enhanced Wireless Consortium und seine Bedeutung für den Wireless Markt

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

Wenn man einmal die abzieht, von denen man eiegntlich gar nicht weiß, was sie machen und die, die ohnehin nicht so wichtig sind, bleiben folgende wesentliche Gruppen übrig, die eine eindeutige Interessenlage haben:

Chiphersteller (Atheros, Broadcom, Intel)
Netzwerk-Komponenten Hersteller (Cisco, D-Link, Gateway ...)
Hersteller von Unterhaltungselektronik (Apple, Mitsubishi, Sony...)

Generell haben viele der Hersteller ein hohes Maß an Interesse am SOHO und Unterhaltungs-Markt. Wie wir wissen, ist es vor allem dieser Markt, der eine schnellere WLAN-Lösung sozusagen hochnotpeinlich händeringend sucht.

Die EWC-Spezifikation soll dazu dienen, WLANs mit hohem Durchsatz, HT-WLANs, beschleunigt zu einer Implementierung zu führen. Dabei gibt es folgende wichtige Ziele:

- Gemischte Interoperabilität mit IEEE 802.11 a,b und g-Netzen für höhere Performance unter gleichzeitiger Beibehaltung der Möglichkeit der Einbindung vorhandener Geräte
- PHY-Datenraten bis 600 Mbit/s. zur Unterstützung von Anwendungen, die das benötigen, wie z.B. HDTV und der generellen Entlastung von Batterien durch kürzere aktive Sendezeiten
- Erhöhte Effizienz der MAC mit Frame Aggregierung. Das soll dem Nutzer mindestens 100 Mbit/s. Nutzdatenrate bringen
- Benutzung von 2,4 GHz oder 5 GHz nach dem bisherigen Frequenzplan der IEEE 802.11-Systeme
- Benutzung von 20 MHz und/oder 40 MHz breiten Sende/Empfangskanälen für höhere Leistung
- Benutzung von bis zu 4 Sende/Empfangsantennen zur Steigerung der Datenrate und der Robustheit des Funksignals mit mehrdimensionaler Orthogonalität
- Größere Reichweite mit mehreren Antennen zur Abdeckung größerer Bereiche mit höherer Leistung

Insgesamt gesehen gibt es weder technische Überraschungen noch wesentliche Neuheiten gegenüber IEEE 802.11n. Im Gegensatz zur vorliegenden Draft Version von IEEE 802.11n ist die EWC-Spezifikation nicht in einer Form geschrieben, die zu einer direkten Erweiterung der vorliegenden Standards IEEE 802.11a,b,g und h führen kann.

Die EWC-Spezifikation greift die wichtigsten Elemente von IEEE 802.11n auf und führt an den Stellen, wo es notwendig erscheint, eine Art Exegese der 802.11n-Spezifikation im Sinne einer besseren Konkretisierung durch. Denn abgesehen davon, dass IEEE 802.11n eine Reihe von Optionen enthält, die noch verhandelt werden müssen, sind auch einige Bereiche mit Absicht nicht so durchformuliert, wie es für eine konkrete Implementierung nötig ist.

Zusammengefasst kann man sagen, dass EWC gegenüber 802.11n die gleiche Rolle einnimmt, wie WiFi damals gegenüber 802.11b. Dass 802.11 zu langsam arbeitet, ist allgemein bekannt. Den EWC-Mitgliedern (allesamt sehr aktive WiFi-Mitglieder) scheint aber auch WiFi zu langsam zu arbeiten. WiFi hat aber momentan auch eine ganze Reihe anderer Baustellen.

Die Situation ist eben momentan so, dass schnelle WLAN-Zellen dringend vom Heim-Markt benötigt werden, die Hersteller auch sofort entsprechende Chips bauen könnten, wenn denn eben die Standardisierung endlich mit den notwendigen Kompatibilitätsdefinitionen aus den Füßen käme. Das kennen wir ja schon seit 10 BASE-T.

Unabhängig davon muss man aber konstatieren, dass EWC im Gegensatz zu 802.11n keine besondere Rücksicht auf den Europäischen Markt nimmt. Um es schlicht zu formulieren: für einen Großteil der EWC-Spezifikationen gilt, dass Geräte, die nach diesen gebaut werden, in Europa mit gutem Grund überhaupt nicht betrieben werden dürfen.

So betrachtet fällt die Sache gegenüber den vollmundigen Presseankündigungen mehr oder minder in sich zusammen.

1. EWC HT PHY-Spezifikation

Direkt in der Einleitung wird gesagt, dass EWC verträglich mit 802.11 a/b/g und j ist. Von h ist keine Rede. Um es vorweg zu nehmen: DFS und TPC findet man im gesamten Dokument ebensowenig. In meinem Artikel zu 802.11n hatte ich auch schon ausgeführt, warum: die Kombination der gekoppelten 20 MHz Kanalpaare zu 40 MHz-Kanälen ist mit DFS nur ausgesprochen schwierig zu vereinbaren. Die hohen Datenraten können nur mit einer gewissen Sendeleistung erzielt werden. TPC ist von daher eine etwas überflüssige Problematik in diesem Zusammenhang.

Bei den Frame Formaten hat EWC gegenüber 802.11n aufgeräumt: es gibt nur noch drei „Legacy“, „Mixed Mode“ und „Green Field“.

Das Enhanced Wireless Consortium und seine Bedeutung für den Wireless Markt

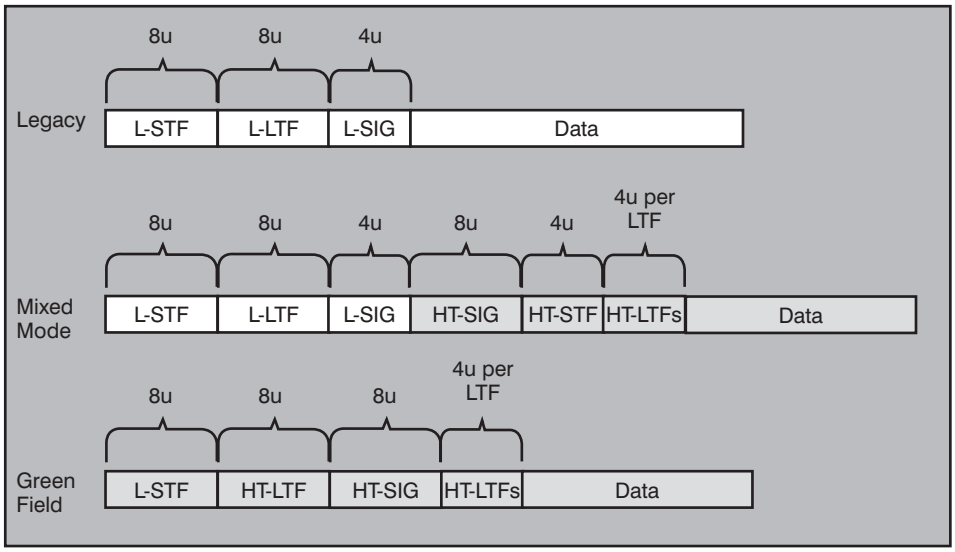


Abb. 1: EWC Frame Formate

Sie unterstützen die drei Modi:

- Legacy Mode: die Pakete werden im „geerbten" 11a oder 11g OFDM-Format übertragen
- Mixed Mode: die Pakete werden mit einer Preambel übertragen, die von 11a und 11g Geräten erkannt werden kann, weil sie aus den kurzen und langen Trainings-Feldern besteht. Der Rest des Paketes hat ein neues Format. Ein Empfänger muss in diesem Mode in der Lage sein, Pakete nach „Legacy" und diese gemischten Pakete zu verarbeiten.

- Green Field: in diesem optionalen Modus werden die Pakete direkt in einem neuen High Throughput-Format ohne Kompatibilitätsvorspann übertragen.

Innerhalb der Frequenzdimension ergeben sich dadurch folgende Alternativen, die verwirrenderweise auch als Modi bezeichnet werden:

- LM: Legacy Mode, äquivalent zu 802.11 a/g

- HT-Mode. Im HT-Mode arbeitet eine Station entweder mit 40 MHz oder 20 MHz Bandbreite mit bis zu vier zeitversetzten Orthogonal-Strömen

- Duplicate Legacy Mode: hier wird in einem 40 MHz-Kanal gearbeitet, der aus zwei 20 MHz-Kanälen zusammengesetzt ist. Auf jedem der 20 MHz-Kanäle wird das 11a-Format benutzt, auf der höheren Frequenz wird es jedoch um 90 Grad gedreht.

- 40 MHz Upper Mode: er wird dazu benutzt, ein Legacy oder HT-Paket im oberen 20 MHz-Kanal eines 40 MHz-Kanals zu schicken

- 40 MHz Lower Mode, analog eben im unteren Kanal.

Für eine Implementierung sind LM und HT-Mode für 1 oder 2 Ströme zwingend.

Der erste Modus ist klar. Der HT-Modus wäre in Europa, wenn überhaupt, nur in der 20 MHz-Variante zulassungsfähig, weil die 40 MHz-Variante eine durchgängige Spektralmaske benötigt, die sich in die bisherigen EU-Kanalpläne absolut überhaupt nicht einfügen lässt. (siehe Abbildung 2)

Harmloser sind da schon die letzten drei Modi, bei denen ein 40 MHz-Kanal aus zwei 20 MHz Kanälen zusammengesetzt wird. Ein Kanalpaar besteht immer aus einem unteren und einem oberen Kanal, wobei der obere Kanal bezogen auf einen herkömmlichen Frequenzplan vier Kanäle höher liegt. Das wäre grundsätzlich für eine Zulassung in Europa geeignet, wenn man es noch mit DFS kombinieren könnte. EWC und 802.11n gehen aber z. Zt von einer relativ starren Kanalvergabe aus, z.B. durch einen Wireless Switch und betrachten das Problem, einem bereits bestehenden Funksignal ggf. ausweichen zu müssen, nicht weiter.

Die letzten zwei Modi erscheinen zunächst unmotiviert. Das ändert sich, wenn man das spezielle Zugangsverfahren betrachtet, was in diesem Zusammenhang benutzt werden soll. Es ist eine vereinfachte Variante des schon längeren Multichannel-DLP Protokolls. Ich hatte es schon vor über zwei Jahren im Rahmen der ersten Überlegungen der High Throughput Study Group vorgestellt. Das Verfahren arbeitet zunächst einmal in einem Kanal traditionell mit DCF. Zwei Stationen können dann aber im Rahmen eines Two-Way Handshakes vereinbaren, die Datenübertragung auf einen weiteren Kanal auszulagern, wobei üblicherweise eine Station eine Art Master-Funktion übernimmt. Das ursprüngliche DLP arbeitete mit einer Auswahl von Kanälen, davon ist jetzt genau ein anderer Kanal übrig geblieben. Der erzielbare Durchsatz ist dann sehr hoch. Probleme treten aber in der vereinfachten Version genau dann auf, wenn mehr als zwei Stationen beschließen, einen anderen Kanal zu benutzen, denn im Gegensatz zum früheren DLP, wo es einfach eine Liste möglicher Kanäle gab, gibt es jetzt eben nur einen.

IEEE 802.11n gibt eine Reihe von unterschiedlichen Methoden an, einen Konflikt

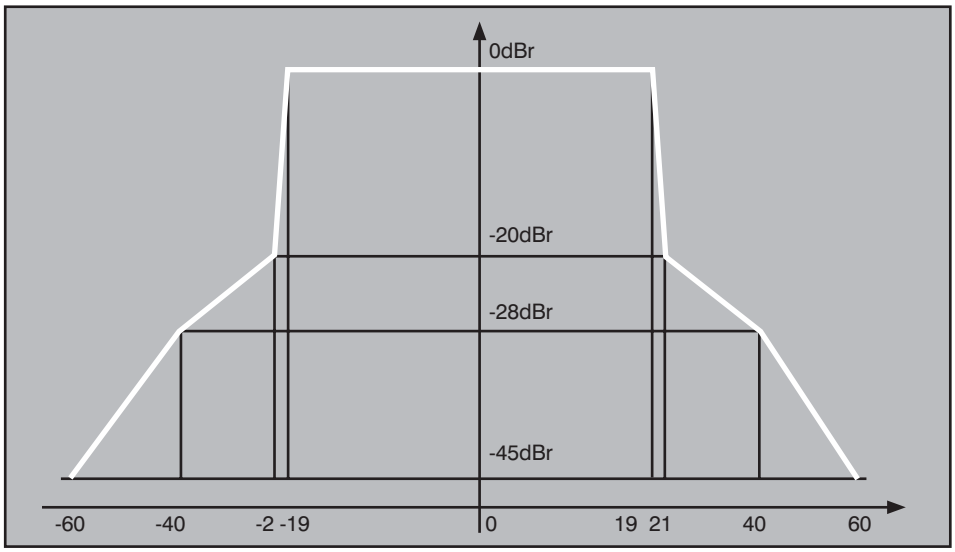


Abb. 2: Spektralmaske für einen durchgängigen 40 MHz-Kanal

Bits 0-6 in HT-SIG1 (MCS index)	Number of spatial streams	Modulation	Coding rate	N_{ES}		N_{SD}		N_{CBPS}		GI = 800ns		GI = 400ns	
				20	40	20	40	20 MHz	40 MHz	Rate in 20 MHz	Rate in 40 MHz	Rate in 20 MHz	Rate in 40 MHz
0	1	BPSK	1/2	1	1	52	108	52	108	6.5	13.5	7 2/9	15
1	1	QPSK	1/2	1	1	52	108	104	216	13	27	14 4/9	30
2	1	QPSK	3/4	1	1	52	108	104	216	19.5	40.5	21 2/3	45
3	1	16-QAM	1/2	1	1	52	108	208	432	26	54	28 8/9	60
4	1	16-QAM	3/4	1	1	52	108	208	432	39	81	43 1/3	90
5	1	64-QAM	2/3	1	1	52	108	312	648	52	108	57 7/9	120
6	1	64-QAM	3/4	1	1	52	108	312	648	58.5	121.5	65	135
7	1	64-QAM	5/6	1	1	52	108	312	648	65	135	72 2/9	150
8	2	BPSK	1/2	1	1	52	108	104	216	13	27	14 4/9	30
9	2	QPSK	1/2	1	1	52	108	208	432	26	54	28 8/9	60
10	2	QPSK	3/4	1	1	52	108	208	432	39	81	43 1/3	90
11	2	16-QAM	1/2	1	1	52	108	416	864	52	108	57 7/9	120
12	2	16-QAM	3/4	1	1	52	108	416	864	78	162	86 2/3	180
13	2	64-QAM	2/3	1	1	52	108	624	1296	104	216	115 5/9	240
14	2	64-QAM	3/4	1	1	52	108	624	1296	117	243	130	270
15	2	64-QAM	5/6	1	1	52	108	624	1296	130	270	144 4/9	300

Abb. 3: Leistung mit 1 und 2 Antennen

16	3	BPSK	1/2	2	2	52	108	156	324	19.50	40.50	21.67	45.00
17	3	QPSK	1/2	2	2	52	108	312	648	39.00	81.00	43.33	90.00
18	3	QPSK	3/4	2	2	52	108	312	648	58.50	121.50	65.00	135.00
19	3	16-QAM	1/2	2	2	52	108	624	1296	78.00	162.00	86.67	180.00
20	3	16-QAM	3/4	2	2	52	108	624	1296	117.00	243.00	130.00	270.00
21	3	64-QAM	2/3	2	2	52	108	936	1944	156.00	324.00	173.33	360.00
22	3	64-QAM	3/4	2	2	52	108	936	1944	175.50	364.50	195.00	405.00
23	3	64-QAM	5/6	2	2	52	108	936	1944	195.00	405.00	216.67	450.00
24	4	BPSK	1/2	2	2	52	108	208	432	26.00	54.00	28.89	60.00
25	4	QPSK	1/2	2	2	52	108	416	864	52.00	108.00	57.78	120.00
26	4	QPSK	3/4	2	2	52	108	416	864	78.00	162.00	86.67	180.00
27	4	16-QAM	1/2	2	2	52	108	832	1728	104.00	216.00	115.56	240.00
28	4	16-QAM	3/4	2	2	52	108	832	1728	156.00	324.00	173.33	360.00
29	4	64-QAM	2/3	2	2	52	108	1248	2592	208.00	432.00	231.11	480.00
30	4	64-QAM	3/4	2	2	52	108	1248	2592	234.00	486.00	260.00	540.00
31	4	64-QAM	5/6	2	2	52	108	1248	2592	260.00	540.00	288.89	600.00
32	1	BPSK	1/2	1	1		48		48		6		6.67

Abb. 4: Leistung mit 3 und 4 Antennen

in diesem Zusammenhang zu lösen. Diese wurden von EWC auf ein paar Holzhammermethoden ausgedünnt, z.B. einfach die Paarung unterer/oberer Kanal zu tauschen, was natürlich zu einer fürchterlichen Unterdrückung aller Stationen führt, die nicht im DLP-Modus arbeiten. Das reicht aber im Grunde genommen auch, denn z.B. im Home Bereich wird es einen derartigen Konflikt kaum geben.

Auf der nächsten Seite sieht man die unter EWC möglichen Modulations- und Codierungsschemata. In den vier rechten Spalten ergeben sich die resultierenden Bandbreiten. Dazu ist natürlich zu sagen, dass

Das Enhanced Wireless Consortium und seine Bedeutung für den Wireless Markt

für Europa nur die 20 MHz-Spalten eine Geltung haben können. Die beiden Spalten ganz rechts gelten für ein gegenüber 802.11a verkürztes Guard Intervall, das ist technisch durchaus machbar. Der etwa 10-prozentige Gewinn gegenüber den Werten der dritten und vierten Spalten von rechts erklärt sich einfach aus einem geringeren Overhead.

Dieses verkürzte Intervall ist die einzige technische Spezialität von EWC gegenüber 802.11n und so kommt man denn auch auf maximal 600 statt bisher 540 Mbit/s. So etwas kann nur von den Chipherstellern kommen, die hier offensichtlich das Problem des OFDM-Trainings besser gelöst haben als bisher. Allerdings klappt das natürlich nur dann, wenn sowohl Sender als auch Empfänger diese höhere Taktung unterstützen.

Bleibt man in einem vernünftigen Vergleichsbereich bis z.B. 2 Antennen und 20 MHz, sind die Gewinne von EWC gegenüber 802.11n marginal, es bleibt bei 130 bzw. 144 4/9 Mbit/s. Vor allem das 4/9 wird entscheidend helfen.

Auch bei EWC konnte man sich nicht zu 256-QAM oder mehrwertiger Vorcodierung durchringen. Hier zeigt sich ganz deutlich, dass man auf Basis bestehender Transceivertechnologie schnell zu Potte kommen möchte und jede wirkliche technologische Erweiterung scheut.

Ein bisschen mutig ist die Abkürzung der Vorcodierung des Signals. Das macht man viel einfacher, als in IEEE 802.11n vorgesehen. Inwieweit dadurch die Signalqualität in einer extremen Umgebung leiden könnte, ist ohne weitere Untersuchung nicht abzusehen. Für ein normales HDTV- , VoIP- oder MP3-Signal ist das allerdings ohnehin bedeutungslos. (siehe Abb. 3 und 4)

2. Die EWC HT-MAC Spezifikation

Diese Spezifikation dünnt die IEEE 802.11n-Spezifikation ebenfalls auf ein eigentlich vernünftiges Maß aus. Im Vordergrund stehen die Funktionen

- Aggregation
- Vereinfachtes Acknowledgement
- Multirate-Support
- Verkürztes Inter Frame Spacing
- Verwaltung der 40 MHz-Kanalpaare

Diese sind i.W. so, wie auch schon in meinem Artikel zu 802.11n beschrieben, allerdings gibt es auch hier eine Ausdünnung von unnützen Sonderfällen, die aber auch bei IEEE 802.11n noch zur Disposition stehen.

Es gibt eine Reihe von starken Vereinfachungen hinsichtlich der Codierungssicherung, also eigentlich lässt man alles bis auf die gute alte CRC weg. Auch hier hat 802.11n wesentlich mehr Ansätze. Ob man diese jedoch wirklich benötigt, oder ob sie nur overheadhaltige Verzierung sind, muss noch diskutiert werden.

3. Chiphersteller, 802.11n und EWC

Den Chipherstellern kommt eine gewichtige Rolle bei der Entwicklung der Komponenten zu, ja eigentlich die absolute Schlüsselrolle. In verschiedenen, meist technisch weniger qualifizierten Presseartikeln werden Mutmaßungen darüber angestellt, welcher Chiphersteller welchem anderen mit welcher Initiative ein Bein stellen möchte. Ich will hier versuchen, das ein wenig auf den Boden der Tatsachen zu bringen und dazu eine Relation zwischen den aktuellen Bemühungen der Chiphersteller und den Initiativen, besonders EWC, herzustellen. Der Markt hat sich in 2005 erheblich bewegt und es gibt Gewinner und Verlierer.

- Gewinner (nach IDC, DellÓro):
  - Broadcom + 44% Wachstum, jetzt Platz 1
  - Atheros + 95% Wachstum, jetzt Platz 2
  - Intel + 57% Wachstum, hält Platz 3
- Verlierer
  - Conexant/Globespan/Virata runter auf Platz 4
  - Texas Instruments verliert Anteile, runter auf Platz 5

Der manchmal erwähnte Chiphersteller Airgo ist statistisch i.W. bedeutungslos.

Bleiben wir also bei den Gewinnern. Hier spielt Atheros eine besondere Rolle.

Dieser Chiphersteller ist sehr aktiv hinsichtlich proprietärer Lösungen für mehr Leistung. Und hat damit durchaus Erfolg. Aktuelle Produkte sind SUPER g für mehr Leistung bei 2,4 GHz, SUPER ag für mehr Leistung bei 2,4 und 5 GHz und Vlocity MIMO für Leistung über 100 Mbit/s. Atheros ist damit gleichzeitig Antrieb und Gefährdung der Standards.

Vlocity MIMO ist ein „vollkompatibler“ MIMO-Ansatz, aber wozu kompatibel, wird nicht gesagt. Letztlich ist es so, dass die Geräte andere Geräte, die Vlocity nicht unterstützen, nicht stören. Anwendungsbereiche sind VoIP, Spiele und HDTV. Im Gegensatz zum IEEE 802.11n gibt es nicht nur mehrere Sende- sondern auch mehrere Empfangsantennen. Man verweist hierbei auf die bessere Unterdrückung von Multipath-Effekten. (siehe Abbildung 5)

Das Enhanced Wireless Consortium und seine Bedeutung für den Wireless Markt

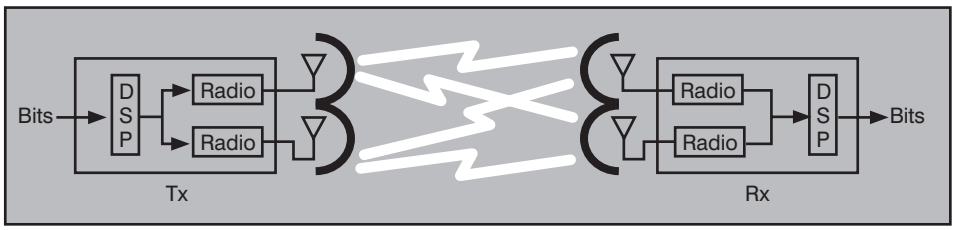


Abb. 5: Atheros Vlocity MIMO

Vlocity MIMO benutzt „Subcarrier Based Maximal Receive Combining“. Die Empfangsantennen werden praktisch zusammen geschaltet, so dass Unterschiede in der Signalstärke, die sich aus den Umgebungsbedingungen ergeben, so gut wie möglich ausgeglichen werden. Das ist anders als Antennen Diversity, wo sich der Empfänger die Antenne aussucht, die das statistisch stärkste Signal bringt und sie dann eine Zeit lang als einzige Antenne benutzt. Bei OFDM kompensiert es nach Aussagen des Herstellers die unterschiedliche Weg-Dämpfung der Unterkanäle. (siehe Abbildung 6)

Damit klärt sich auch die „Kompatibilität“: ein Empfänger kann das Signal auch empfangen, wenn er nur eine Antenne hat, dann eben ohne den zusätzlichen Gewinn. Da im Gegensatz zu IEEE 802.11n auf der Sendeseite keine Multiplextechnik eingesetzt wird, sondern beide Antennen das Gleiche abstrahlen, können 11 a, b oder g-Stationen mit dem Signal trotzdem etwas anfangen. Das geht bei 802.11n nicht!

Ein weiterer Trick ist die Verwendung einer geeigneten Phasenverschiebung. Versetzt man identische OFDM-Signale in der Phase, kann man die Gesamt-Empfangsleistung integrativ erhöhen, theoretisch bis zur Größenordnung des Quadrats der Anzahl der Sende-Antennen. Bei zwei Antennen also bis zur vierfachen Leistung einer einzelnen Antenne. Die Leistung an der Sendeantenne muss dazu nicht erhöht werden, der Effekt ergibt sich durch Leistungssummation der phasenverschobenen Signale in der Luft. Dieses Verfahren gehört seit über 30 Jahren zu den Basistricks der MIMO-Technologie.

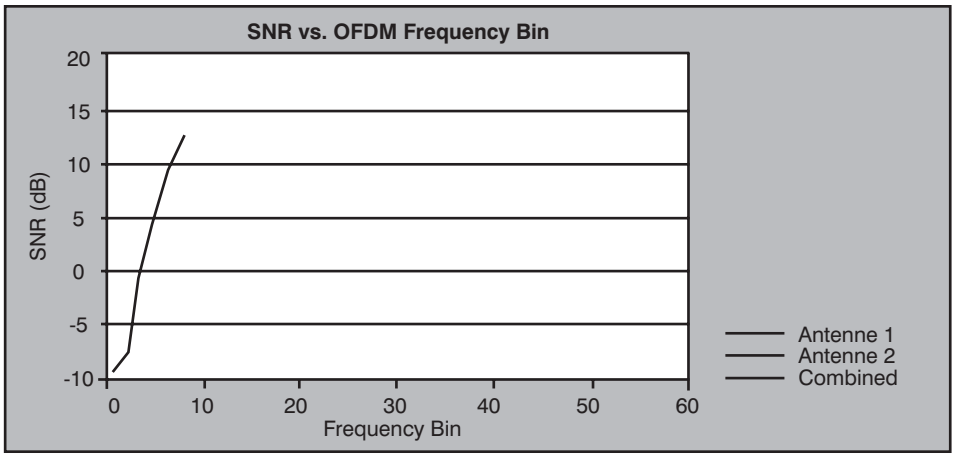


Abb. 6: Kompensation der OFDM-Wegdämpfung

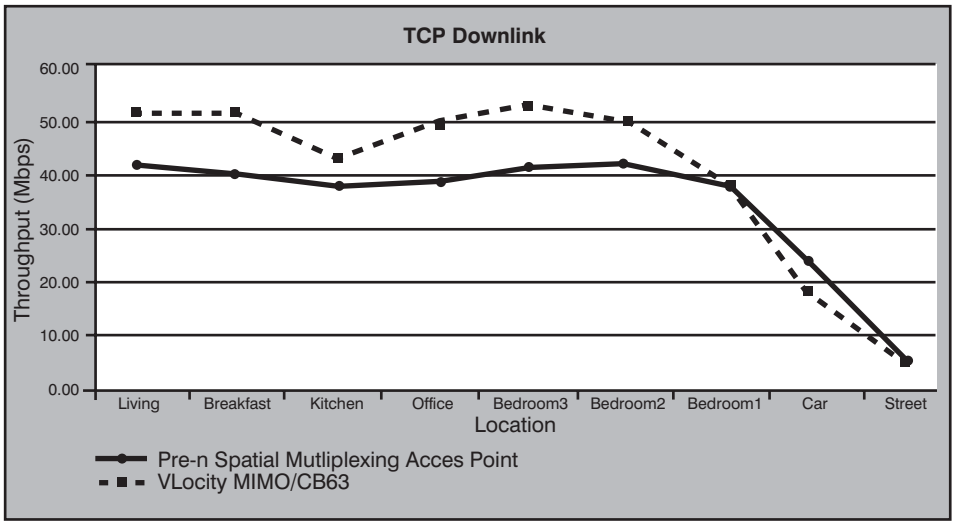


Abb.7: TCP-Downlink-Leistung für „Pre-n“ vs. Vlocity nach Angaben des Herstellers

Auch das ist wieder „kompatibel“ zu 11a, b und g, weil die Empfänger leichte Phasenverschiebungen durch Selbstsynchronisation ausgleichen können. Nochmal zum Nachrechnen: zwei Antennen, die mit jeweils der erlaubten Ausgangsleistung senden, verdoppeln diese an der Sendeseite. Durch die Phasenverschiebung wird erreicht, dass die zwei Empfangsantennen jeweils „voll“ arbeiten und damit der Bruchteil der ankommenden Sendeleistung verdoppelt wird. Damit wird die ankommende Sendeleistung insgesamt vervierfacht. Wird durch die Regulierung oder andere Überlegungen die Sendeleistung als Summe auf einen Wert begrenzt, ergibt sich immer noch die mögliche Verdoppelung der Eingangsleistung auf der Empfängerseite. Und das Ganze natürlich mit sehr bescheidenem zusätzlichem Aufwand.

Das Vlocity Prinzip kann für 802.11 a, b und g gleichermaßen benutzt werden. Empfänger mit mehreren Antennen können von der zusätzlichen Leistungsausbeute profitieren. Letztlich wird die Reichweite für die Übertragung mit hohen Geschwindigkeiten vergrößert. Empfänger mit nur einer Antenne profitieren immer noch ein bisschen wenn mit zwei Antennen phasenversetzt gesendet wird.

Dies steht im Gegensatz zu IEEE 802.11n, wo nur 11n-Stationen im „11n-Modus“ mit zweidimensionaler Orthogonalität untereinander kommunizieren können.

Im IEEE 802.11n ist nur eine Empfangsantenne bei mehreren Sendeantennen vorgesehen. Die Anwendung mehrerer Empfangsantennen im Vlocity-Modus kann einen leichten Gewinn bringen, allerdings darf man den Phasenverschub nicht mit der zweidimensionalen Orthogonalität mischen, das funktioniert definitiv nicht.

Die durchschnittlichen Gewinne liegen je nach Kombination zwischen 3 und 6 dB. Das ist relativ viel, vor allem, wenn man bedenkt, dass im SOHO-Bereich kaum mit Richtantennen gearbeitet werden kann, sondern die „Rundstrahlflächenab-

deckung“ im Vordergrund steht. (siehe Abbildung 7)

Insgesamt kann sich der Hersteller auf dem interessanten SOHO-Markt durchaus einen Vorsprung herausarbeiten, weil es dem Anwender letztlich nur darauf ankommt, möglichst viel Leistung aus ElNEM Access Point herauszuholen.

In Gegensatz zu echten 11n-Produkten ist das jetzt so lieferbar und kann in Home-Equipment verbaut werden. Größter Vorzug ist, dass auch Geräte nach anderen Standards versorgt werden können. Der Erfolg von 11g zeigt, WIE UNGEDULDIG der Markt ist. Selbst in einem Slot von nur 12 Monaten könnten sie sich mit dieser Lösung dumm und dämlich verkaufen. Bei einem Mehr-Zellen-Design ist von der Theorie her nicht durch eine Zunahme von Störungen in einer Fremd-Zelle durch Vlocity-APs zu rechnen, praktisch müsste man das noch nachmessen. Von einer späteren 11n-Lösung werden die Vlocity-Stationen behandelt wie alle anderen 11 a,b,g,h-Stationen: sie werden untergebuttert!

In der EWC-Spezifikation finden sich ganz wesentliche Elemente von Vlocity wieder. Atheros ist also ganz klar ein Gewinner, wenn diese Spezifikation einen Durchbruch erzielt. Andererseits würde ich an Stelle des Herstellers ja auch verzweifeln, wenn ich fertige 100 Mbit/s.-Lösungen hätte, die offensichtlich funktionieren, aber von der Standardisierung bislang nur unangemessen berücksichtigt wurden.

Broadcom ist nach IDC am schnellsten wachsender Enterprise IP Phone Chip Supplier. Aber auch sonst nicht untätig, denn im August 2005 wurde der 75 Millionste NetXtreme GbE Controller hergestellt. Broadcom ist erster Hersteller für Single Chip WiFi. Besonders chic ist der BCM 1160 Mobile Voice Processor. Mit ARM9 CPU, integriertem Voice-Band Codec mit Direktmikro und hoher Ausgangsleistung im Low Power Design und nahtloser Integration zu WLAN-Chips schafft er das WiFi Phone Reference Design: BCM 1160 + BCM 4318. BCM 4318 ist ein Single Chip 11 b/g Baseband/MAC/Radio. Damit ist Broadcom erster Hersteller mit Zwei-Chip Design für VoWLAN. Die CMOS-Radios sind preiswert und benutzen komplexe DSP-Algorithmen, die in jeder Richtung ausbaubar sind.

Broadcom ist sehr fleißig bei IEEE 802.3an und IEEE 802.11. Die sog. Xpress Technologie verbessert den Durchsatz durch Rückgriff auf alte 802.11-Features, die bei den Neudefinitionen in Vergessenheit geraten waren. Wesentlich ist auch das Frame Bursting: eine Station muss normalerweise nach der Sendung eines Pakets eine Pause machen und sich dann für das nächste Paket mit den anderen wieder um den Kanal schlagen. Mit Frame Bursting darf sie mehrere Pakete hintereinander absetzen.

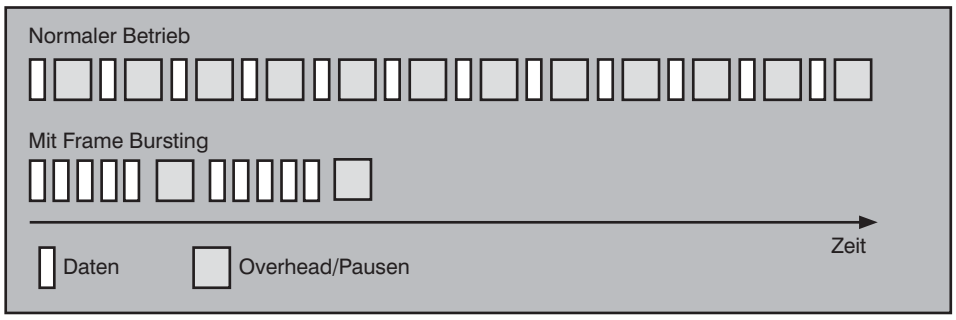


Abb. 8: Frame Bursting

Bisher war diese Eigenschaft nicht so interessant, aber grade hinsichtlich der Problematik der VoIP-Samples und der Notwendigkeit eines APs, an alle in der Zelle aktiven Phones möglichst gleichzeitig Samples abzusetzen, rückt die in den Vordergrund.

Es ist NICHT proprietär! Broadcom kann nichts dafür, wenn andere Hersteller dieses ältere optionale 802.11-Feature nicht implementiert haben. Hat man nur einen AP mit Xpress, kann der das Downstream nutzen, weil ja alle immer empfangen können, wenn sie nicht grade selbst senden. Nicht mit Xpress ausgestattete Stationen können trotzdem wie gewohnt kommunizieren. Es funktioniert schon mit a,b und g. Dafür gibt es Produkte. Frame Bursting ist von IEEE 802.11e wieder aufgegriffen worden und heißt dort Continuation Transmit Opportunity CTXOP

Frame Bursting kann mit Fragment Bursting kombiniert werden. Fragment Bursting bedeutet im Kern, dass die Performance Vorteile nicht nur auf Einzelpakete, sondern auch auf Segmente (segmentierter) Einzelpakete übertragen werden können.

Frame Bursting ist auch Bestandteil der von Broadcom und Microsoft gespushten WiFi Multimedia Extensions, einer (sinnvollen!) Teilmenge der IEEE 802.11e QoS-

Spezifikationen. Der Leistungsgewinn mit Xpress bei 11g ist ca. 23 - 27 %, der Leistungsgewinn mit Xpress bei 11b: bis ca. 75%.

Ebenfalls interessant ist die sog. OneDriver Software der AirForce Produktfamilie, z.B. verbaut von Apple, Dell, HP, Linksys (Cisco).

Intel hat einen dicken Fuß im Markt durch die Centrino-Technologie, ist aber eigentlich ziemlich leidenschaftslos, was die WLANs als solche und als Teilmarkt angeht. Man möchte nur immer neue Standards schnell integrieren. Generell anders ist die Situation bei WiMAX: der ausgesprochen interessante Provider-Markt soll mit dieser Technologie beflügelt werden.

Nach diesen Betrachtungen sollte klar geworden sein:

EWC ~ Vlocity + Xpress + ein bisschen Verzierung

Die momentan absoluten Marktführer Atheros und Broadcom können in der EWC-Spezifikation ihre speziellen, bereits seit längerer Zeit funktionsfähigen Lösungen Vlocity für die PHY und Xpress für die MAC kombinieren und schaffen damit in einer Art großen WLAN-Koalition ein Gegengewicht zu der in den letzten 18 Monaten allzu zaghaften IEEE 802.11n-Bewegung ohne die Standardisierung an sich zu beschädigen. Das verdient, wenn sie es so durchziehen können, schlichtweg das Prädikat GENIAL.

Die anderen EWC-Teilnehmer profitieren dadurch erheblich, weil sie viel schneller zu WLANs mit mehr als 100 Mbit/s. kommen und in ihre Produkte integrieren können, als das auf dem „normalen“ Weg möglich wäre.

4. Zusammenfassung und Bewertung

EWC ist alles in allem eine plausible Untermenge von IEEE 802.11n, denn zu 95% wird hier nur aufgeräumt, gestrafft und vereinfacht. Die einzige wirklich technische Abweichung und Erweiterung ist die gestraffte Vorcodierung, die zu 10% mehr Nominalleistung führt.

EWC macht keinen Unterschied zwischen 2,4 und 5 GHz. Lässt man es aber in einer 802.11 g Umgebung laufen, werden die bisherigen Stationen heftig untergebuttert, einmal durch die Modifikationen des Steuerungs-Verfahrens und zum anderen durch die Kanalbündelungen. 802.11b-Stationen können an dem ganzen definitiv nicht mehr teilnehmen, weil sie das OFDM-Trainingssymbol nicht verstehen. Offensichtlich sieht EWC 802.11b als aussterbende Technologie.

In einer 5 GHz-Umgebung gibt es in Europa Probleme wegen des Fehlens von DFS und TPC. Man muss einfach abwarten, ob und wie die Hersteller das Problem lösen. Die Verwendung von durchgängigen 40 MHz-Kanälen zerstört alles, was wir bislang so planen. Die Verwendung von 2 X 20 MHz Kanalpaaren wäre möglich, vor allem, wenn es mit 802.11h DFS kombiniert wird, wobei die Stationen der älteren Variante einfach vornehm ausweichen. 802.11 a/h und EWC-Stationen in einem gemeinsamen Kanal sind zwar möglich, aber auch hier werden die Stationen nach älterem Standard schwer in ihren Möglichkeiten beschnitten.

EWC ist sicherlich ganz prima im Soho-Bereich, auch wenn die Leistung bei den Basisversionen bescheiden bleibt. Für den Enterprise-Bereich ist es nur dann wirklich brauchbar, wenn die gesamte Kanalverwaltung dynamisiert und zentralisiert wird, z.B. mit einem Wireless Switch.

Die wesentlichen Chiphersteller sind so weit, dass sie eigentlich schon zum Weihnachtsgeschäft 2005 loslegen können. Es würde mich nicht wundern, wenn wir in den USA wirklich noch in diesem Jahr die ersten Home Entertainment-Komponenten mit 130 oder 150 Mbit/s. WLAN-Technik sehen.

Festzuhalten ist aber auch, dass EWC gegenüber IEEE 802.11n keinerlei wirkliche Verbesserungen in der reinen Funktechnik bringt. Erst mit 256 QAM und mehrwertiger Codierung sind weitere Leistungssprünge denkbar.

EWC ist also nichts anderes als ein weiteres Glied in der Kette der schnell vergänglichen WLAN-Standards. Es wird zumindest im Home-Bereich 2006 und 2007 dominieren und danach schon wieder von Standards für Gigabit-Zellen mit mindestens echten 500 Mbit/s. in der Zelle abgelöst werden.

Report des Monats

Neuerscheinung
Enterprise WLANs erfolgreich planen und betreiben

Lesen Sie im Folgenden einen Ausschnitt aus der Studie „Enterprise WLANs erfolgreich planen und betreiben“.

Anforderungen an WLANs im Enterprise-Bereich

WLANs im Enterprise-Bereich zeichnen sich typischerweise durch die folgenden zu Grunde liegenden Anforderungen aus:

- Nutzung des 5-GHz-Bereichs: Mit der steigenden Nutzung von WLANs ist das knapp bemessene Frequenzspektrum bei 2,4 GHz oft hoffnungslos überbelegt durch eigene WLAN-Anwendungen, fremde WLAN-Anwendungen, die in die eigenen Bereiche hinein strahlen, und Fremdsysteme. Der Wunsch nach einem erweiterten Spektrum ist daher verständlich. Hierzu ist eigentlich der 5-GHz-Bereich gedacht.

- Trennung von WLAN und LAN: Das WLAN Distribution System wird logisch oder physikalisch von der LAN-Infrastruktur getrennt realisiert. Die Verbindung zwischen WLAN Distribution System und LAN erfolgt über einen zentralen Übergabepunkt, der das WLAN abschließt und typischerweise Sicherheitsfunktionen realisiert (z.B. Firewall-Funktionen). Bei großflächigen WLANs ist eine logische Trennung aus wirtschaftlichen Gründen oft die bevorzugte Alternative. Hier ist die Kernanforderung, dass sich das WLAN Distribution System nahtlos in ein bestehendes LAN-Konzept integriert. Mit anderen Worten bedeutet diese Forderung, dass sich ein WLAN auf einer „beliebigen“ LAN-Infrastruktur ohne Probleme realisieren lässt und trotzdem die geforderte logische Trennung zwischen LAN und WLAN bestehen bleibt.

- Kapazitätsorientierte flächendeckende Zellplanung: Die Funkversorgung erfolgt (weitestgehend) flächendeckend durch überlappende Funkzellen. Der Grad der Überlappung bestimmt wesentlich die Redundanz und damit die Verfügbarkeit des WLANs. Die Dimensionierung und Positionierung der Funkzellen (d.h. Auswahl und Positionierung der Antennen und Festlegung

der effektiven Sendeleistung) geschieht insbesondere in Abhängigkeit vom geforderten Verkehrsvolumen und der erwarteten Clientdichte pro Raumeinheit.
- Trennung von Benutzergruppen: Eine flächendeckende WLAN-Versorgung stellt eine gemeinsame physikalische Infrastruktur für alle drahtlosen Anwendungen zur Verfügung. Die Konsequenz ist typischerweise aus Gründen der Sicherheit die Forderung nach einer logischen (ggf. sogar physikalischen) Trennung von Benutzergruppen. Die einzelnen Benutzergruppen können unterschiedlichen Sicherheitsniveaus zugeordnet sein und die Absicherung der WLAN-Kommunikation erfordert ggf. unterschiedliche Methoden für verschiedene Nutzergruppen.

- Online-Mobilität: Clients können unabhängig vom Aufenthaltsort an einer beliebigen Position mit WLAN-Abdeckung eine Netzverbindung aufbauen, ohne dass hier eine spezielle manuelle Konfigurierung durch den Nutzer erforderlich ist. Innerhalb des Versorgungsgebiets kann ein Client sich bewegen, ohne dass die Verbindung aus dem Blickwinkel des Clients auf Layer 3 abbricht.

- Roaming-Fähigkeit: Bei einem Wechsel von WLAN-Geräten (Notebooks, PDAs, Smart Phones, etc.) zwischen Standorten eines Unternehmens oder einer Behörde muss es möglich sein, dass am besuchten Standort der Nutzer ohne Eingriff in die Konfiguration des Clients über das dortige WLAN Dienste (ggf. mit Einschränkungen aus Gründen der Absicherung zwischen Standorten) genutzt werden können.

- Gastzugang: Für Projekte, in denen Teams firmen- bzw. behördenübergreifend zusammengestellt werden, bedeutet ein Gastzugang zum Internet für Fremdfirmenmitarbeiter oft eine erhebliche Arbeitserleichterung. Hier ist ein Gastzugang über ein WLAN oft das Mittel der Wahl, da das WLAN flächendeckend angeboten werden kann und Kontrollmechanismen zur effektiven Trennung vom LAN und den über das LAN erreichbaren Ressourcen zur Verfügung stehen.

- Zentrales Management: Access Points werden als zusätzliches Netzelement in das zentrale Netzmanagement übernommen. Die Luftschnittstelle ist mit besonderer Aufmerksamkeit zu überwachen, da sie die eigentlich kritische Ressource darstellt.

Gerade der erste Punkt des Aufbaus eines WLANs auf einer nahezu beliebigen LAN-Infrastruktur unter Beibehaltung einer logischen Trennung von WLAN und LAN, verbunden mit der Forderung einer flächendeckenden Mobilität stellt hohe Anforderungen an die WLAN-Technik, die hier schnell an die Grenzen der im IEEE 802.11-Standard und seinen Erweiterungen spezifizierten Mechanismen stößt.

Nutzung des 5-GHz-Bereichs

Im 5-GHz-Bereich müssen (im Vergleich zum ISM-Band bei 2,4 GHz) speziell in Europa erhebliche Regulierungsauflagen eingehalten werden, um das vollständige zur Verfügung stehende Spektrum mit einer brauchbaren Sendeleistung nutzen zu dürfen. Es sind jedoch bereits diverse Systeme verfügbar, die den Vorgaben der Bundesnetzagentur (ehemals Regulierungsbehörde für Telekommunikation und Post, RegTP) hinsichtlich Transmit Power Control (TPC) und Dynamic Frequency Selection (DFS) genügen und daher alle 19 im 5-GHz-Band verfügbaren Kanäle nutzen können. Ein angenehmer Be-

gleiteffekt von DFS ist in diesem Zusammenhang, dass der Netzplaner sich nicht mehr um die Vergabe der Kanäle an die einzelnen Access Points kümmern muss. Das erledigt das System von alleine.

Die Kernanforderungen sind nun: Die Interoperabilität für Geräte, die DFS und TPC unterstützen, muss sichergestellt werden und IEEE 802.11a sowie IEEE 802.11h müssen von Endgeräten unterstützt werden. Gerade im Endgerätebereich liegt hier das Problem, dass hier Standards oft erst sehr spät umgesetzt werden. Nachdem eine Funktion in einem Chipsatz zur Verfügung steht, wird diese Funktion in einem zweiten Schritt in den Access Points angeboten. Danach folgen die Standard-Client-Adapter (z.B. für Notebooks) und erst mit großem Abstand werden die Funktionen in Spezialsysteme (z.B. VoIP WLAN-Handsets) integriert.

Trennung von WLAN und LAN

Es gibt mehrere Gründe, die für eine Trennung von WLAN und LAN sprechen:
Werden Access Points ohne zusätzliche Maßnahmen direkt an das LAN angeschlossen, besteht zunächst das Problem, dass mit jedem Access Point eine potentielle Sicherheitsschwachstelle verbunden ist. Also entsprechen zum Beispiel 100 Access Points auch 100 Schwachstellen im LAN, über die ein direkter Zugang zu den am LAN angeschlossenen Ressourcen möglich ist. Natürlich kann hier mit entsprechenden Sicherheitsmechanismen entgegen gewirkt werden. Beispielsweise könnte der Zugang über die Access Points mit modernen Sicherheitsmechanismen wie WPA-Enterprise oder WPA2-Enterprise abgesichert werden, und vom Sicherheitsniveau entspräche dann der Clientzugang über das WLAN mindestens dem des kabelbasierten Clientanschlusses. Trotzdem ist dies unbefriedigend, denn auf der WLAN-Seite ist mit einer schwer zu kontrollierenden Vielfalt an unterschiedlichen Endgeräten und Client-Adaptern zu rechnen.

Weiterhin ist bei einem WLAN von einer dynamischen Anzahl von Clients pro Access Point auszugehen. Zudem ist ein WLAN stets ein potentielles Angriffsziel von Außen. Wie man es dreht und wendet, ein Netzwerkport an dem ein Access Point angeschlossen ist, ist einem anderen Sicherheitsbereich zuzuordnen und muss anders behandelt werden als ein Port für den kabelbasierten Client-Anschluss.

Eine Trennung von WLAN und LAN ist nicht nur aus Sicherheitsgründen nahe gelegt. Beispielsweise ist die gewählte Architektur des Distribution Systems zunächst nicht notwendig verträglich mit dem LAN-Konzept. Ob letztendlich ein WLAN als VLAN auf einer bestehenden LAN-Infrastruktur realisiert wird, oder eine vollständig separate physikalische Infrastruktur aufgebaut werden sollte, kann nur im Einzelfall entschieden werden. Entscheidend ist jedoch die Schaffung eines zentralen Übergabepunkts („Single Point of Control“) zwischen WLAN und LAN. Je nach verwendeter Methode zur Absicherung des WLANs geschieht die Trennung am Übergabepunkt zumindest auf Layer 3. Typisch sind an dieser Stelle aber auch ein Abschluss des WLANs mit einem Netzelement mit Firewall- oder VPN-Gateway-Funktion (siehe Abbildung 1).

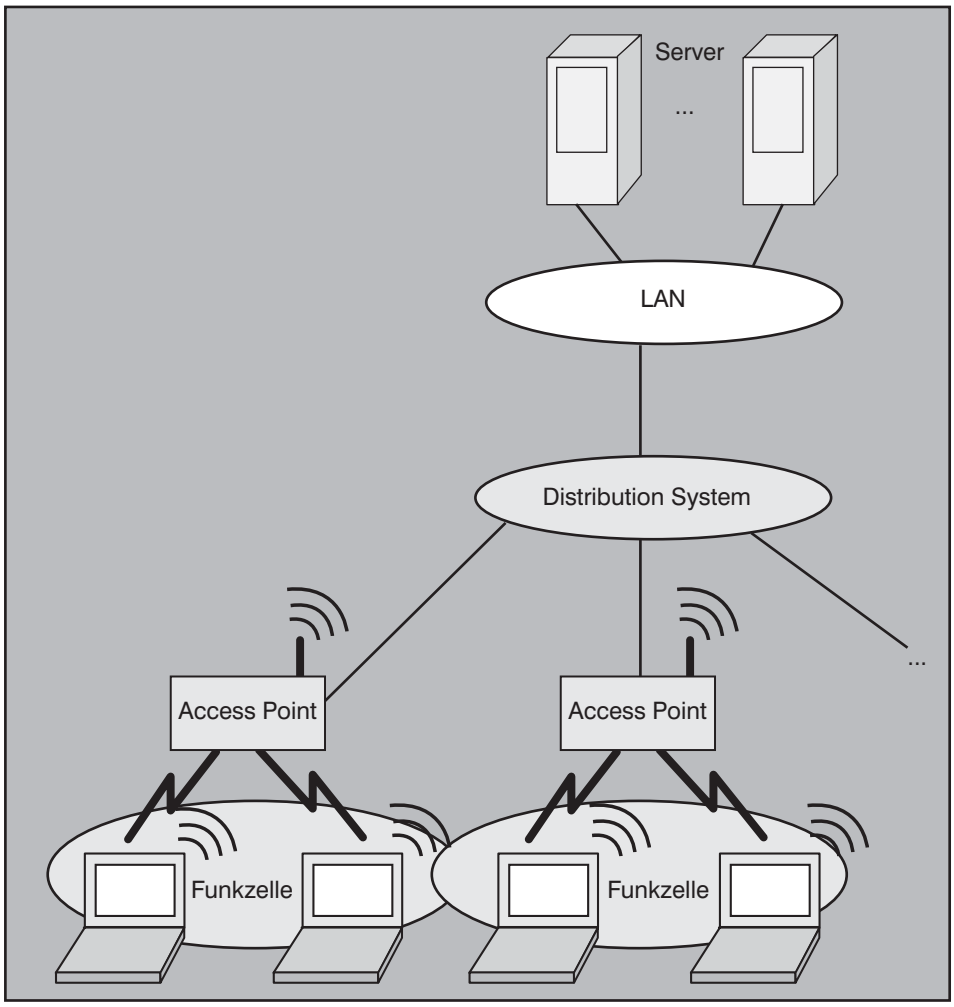


Abbildung 1: Trennung von WLAN und LAN

Kapazitätsorientierte flächendeckende Zellplanung

Der Skalierbarkeit setzen die möglichen Sendeleistungen und insbesondere die Anzahl von überschneidungsfreien Kanälen Grenzen. Dahinter steckt eine einfache Rechnung: Je mehr Kanäle verfügbar sind, desto mehr Funkzellen können sich (vollständig) überlappen, ohne dass es zu Interferenzen kommt, und damit steigt die Kapazität pro Raumeinheit. Bei IEEE 802.11b mit seinen drei Kanälen ist es oft schon schwierig genug überhaupt eine geeignete interferenzreduzierte Kanalzuteilung in der Fläche festzulegen. Die Verwendung von IEEE 802.11g ändert an dieser Situation nichts. Die Kapazität lässt sich hier also nur durch kleinere Funkzellen erhöhen (siehe Abbildung 2).

Trennung von Benutzergruppen

Verbunden mit der Schaffung einer einheitlichen flächendeckenden WLAN-Infrastruktur ist meist die Frage der Zugriffsberechtigungen und der Trennung unterschiedlicher Nutzergruppen. Einem Besucher einer Fremdfirma möchte man vielleicht einen Guest Account anbieten, damit er oder sie auf das Internet zugreifen kann, etwa um über ein VPN auf Email und andere Dienste zuzugreifen. Hier wird das WLAN plötzlich zum firmeninternen Hotspot. Für einen lokalen Mitarbeiter sollten dagegen alle notwendigen lokalen LAN-Ressourcen zur Verfügung stehen. Beide Gruppen nutzen die gemeinsame

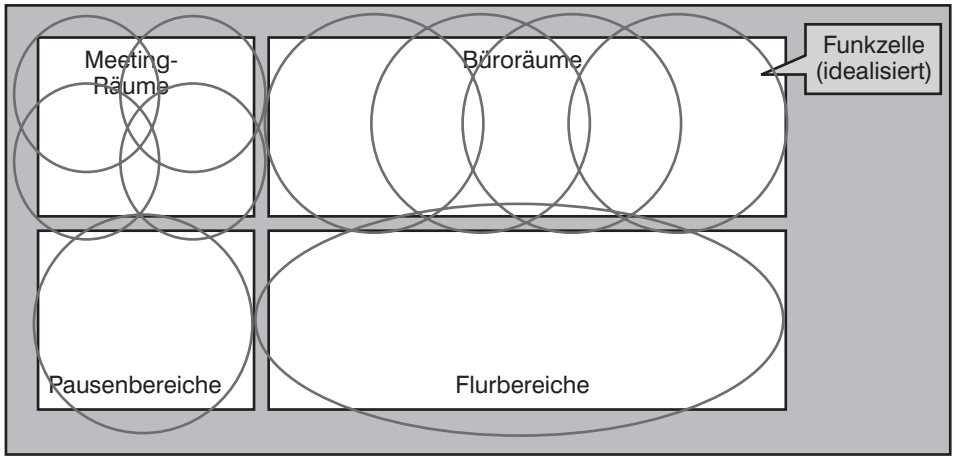


Abbildung 2: Verkehrsorientierte Zellplanung durch unterschiedlich große Funkzellen bzw. unterschiedlich großen Überlappungsgrad zwischen den Funkzellen

WLAN-Ressource, benötigen jedoch unterschiedliche Sicherheitsmechanismen. Während für den Guest Account vielleicht ein unverschlüsselter Zugang über User ID und Passwort genügt, müssen es für den (uneingeschränkten) Zugang zu LAN-Ressourcen schon weitergehende Sicherheitsmechanismen sein.

Eine ähnliche Situation findet man in Bereichen der Produktion und Lagerhaltung. Hier werden oft sehr einfache Endgeräte eingesetzt, die außer WEP keine erweiterten Sicherheitsmechanismen unterstützen. Typisches Beispiel sind Handhelds mit Barcode Scanner. Diese Endgeräte erfordern nur den Zugriff auf dedizierte Server. Daneben werden in diesen Bereichen jedoch zunehmend auch konventionelle Notebooks eingesetzt, um beispielsweise von einem Büro in einer Produktionshalle aus Ressourcen im Bürobereich zu nutzen.

Auch hier sind zwei Benutzergruppen mit unterschiedlichem Sicherheitsniveau zu trennen.

Die Alternative einer physikalischen Trennung durch mehrere separierte WLANs ist bei 2,4 GHz meist nicht praktikabel, da die verfügbare Anzahl von überlappungsfreien Kanälen nicht ausreicht. Generell möglich ist die physikalische Trennung unterschiedlicher Benutzergruppen unter (zusätzlicher) Verwendung von WLANs nach IEEE 802.11a bzw. 802.11h. Befriedigend ist diese Lösung allerdings nicht, einerseits aus wirtschaftlichen Gründen und andererseits, da sie vergleichsweise verschwenderisch mit dem knappen Frequenzspektrum umgeht. Die Fortsetzung des VLAN-Konzepts auf die Luftschnittstelle zur Trennung von Nutzergruppen ist also wünschenswert. Damit verbunden ist auch die Forderung nach einer Bandbreitenkontrolle (und damit nach QoS) für die unterschiedlichen „Wireless VLAN“.

Online-Mobilität

Typischerweise wird das Distribution System für ein WLAN als flaches Layer-2-Netz aufgebaut, um eine uneingeschränkte Mobilität im Versorgungsgebiet zu erreichen. Als Konsequenz findet man WLANs im Einsatz, bei denen sich durchaus 1000 (und mehr) Stationen und Netzelemente in einer Broadcast-Domäne tummeln. Da als Redundanzmechanismus im Distribution System nur Spanning Tree in Frage kommt, beobachtet man solche Entwicklungen natürlich mit ausgesprochenen Bedenken. Die Realisierung eines Distribution Systems als Layer-3-Netz bzw. eines Roaming zwischen Distribution Systems ist jedoch mit vielen Tücken verbunden. Nehmen wir an, beim Übergang von einer Funkzelle zur anderen gelangt ein Client in ein anderes IP-Subnetz. Auf Layer 2 sorgt das WLAN dafür, dass der Zellwechsel ohne Verbindungsabbruch vonstatten geht. Nur passt jetzt nicht mehr die IP-Adresse des Clients, und alle Pakete, die noch für den Client unterwegs sind, werden zunächst noch zum alten Standort geroutet. Verbindungsabbrüche auf höheren Protokollebenen, gegebenenfalls verbunden mit dem Neustart von Anwendungen oder sogar dem Client-System, sind die Folge. Akzeptiert man dies, genügt die Verwendung von DHCP, sofern die Clients DHCP unterstützen, was nicht immer der Fall ist (z.B. manche Barcode Scanner). Andernfalls bleibt keine Wahl, Mobilität muss auf Layer 3 und damit außerhalb von IEEE 802.11 unterstützt werden. Hier gibt es nur zwei Alternativen: (Proxy) Mobile IP oder die noch proprietären Lösungen in Wireless Switches....

Neue Seminarreihe 2006

Quality of Service - QoS

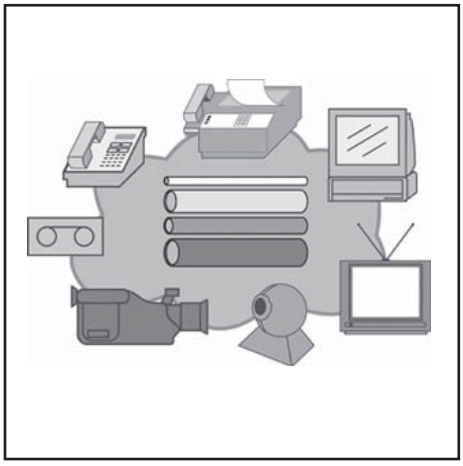
Die ComConsult Akademie veranstaltet vom 14.- 15. Februar 2006 erstmalig ihre neue Seminarreihe „Quality of Service - QoS“ im Holiday Inn am Stadtwald in Köln.

Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standrads es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert.

IP-Netze übertragen bisher im Wesentlichen Daten im Rahmen von robusten Anwendungen, die auf Paketverlust, Verzögerung und reduzierte verfügbare Bitrate relativ tolerant reagieren. Neu sind jedoch Anwendungen wie Voice over IP, industrielle Kommunikation, Gebäudeleittechnik, Videoüberwachung und Gefahrenmanagement, die sich von den bisherigen Applikationen unterscheiden. Diese Anwendungen erfordern:

- Die Einhaltung einer maximalen Signalübertragungszeit (Delay)
- Eine Bandbreiten-Garantie
- Die Einhaltung einer maximalen Schwankung der Signalübertragungszeit (Jitter)
- Eine weitgehend verlust- und fehlerfreie Übertragung

Die Hersteller von Netzkomponenten arbeiten seit Jahren an Lösungen für die Sicherstellung der QoS. Viele dieser Lösungen sind aufgrund ihrer Komplexität bereits verworfen worden. Auch im Fall des einfachsten QoS-Modells der differenzierten Behandlung von wenigen Verkehrsklassen ist eine komplexe Konfiguration von Netzkomponenten erforderlich.



Ist jedoch die Strategie des „Überangebots“ an Netzkapazität aufgrund der technischen und wirtschaftlichen Rahmenbedingungen nicht umsetzbar, führt an QoS-Maßnahmen kein Weg vorbei.

Der Inhalt im Detail:

Sicherstellung von Qualitätsparametern durch Überangebot an Netzkapazität
- wie leistungsfähig muss ein Netz zu dimensionieren, damit auf QoS verzichtet werden kann?
- welche Parameter sind zu messen und zu überwachen?
- ist eine Berechnung der Netzdimensionierung möglich?

Messergebnisse
- Messungen in LAN / WAN / WLAN
- Bestätigen die Messergebnisse die theoretischen Erkenntnisse?

Quality of Service im drahtgebundenen LAN
- QoS in IEEE 802.1D
- QoS in IEEE 802.1Q
- Empfehlungen von IEEE

Der Standard Differentiated Service (DiffServ) und sein Stellenwert
- DiffServ-Architektur
- DiffServ-Implementierungen in Produkten

Quality of Service in WAN
- QoS-Funktionen von Routern
- Strategien bei der Behandlung von Warteschlangen in Routern

Quality of Service bei Multi-Protocol Label Switching (MPLS)
- QoS in MPLS-Standards
- Abbildung von QoS bei IP auf QoS bei MPLS

QoS-Angebote der Service Provider
- Gemeinsamkeiten
- Unterschiede
- Überprüfung von QoS als Bestandteil von Service Level Agreements

Quality of Service bei Wireless LAN (WLAN)
- IEEE 802.11e
- WiFi Multimedia (WMM)
- Proprietäre QoS-Implementierungen

QoS für Voice over IP
- QoS bei VoIP über WAN
- Behandlung von Hard Phones
- Behandlung von Softphones

Durch das Seminar führt Sie Dr.-Ing. Behrooz Moayeri der ComConsult Beratung und Planung GmbH.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Quality of Service - QoS

☐ Ich buche das Seminar
Quality of Service - QoS
vom 14.02. - 15.02.06 in Köln
zum Preis von € 1.390,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Schwerpunktthema

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

Teil 1

Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Mobilität

Mitarbeiter oder mobile Fortbewegungsmittel (Polizei-, Feuerwehr-Fahrzeug, Schiffe, Züge, Gabelstapler) bewegen sich innerhalb engerer oder weiterer Standortbereiche und wollen flächendeckend mit Laptop, PDA, Mobiltelefon (sei es GSM oder WLAN) über einen Zugang zu Daten und Diensten verfügen. Hinsichtlich VLAN- und IP-Subnetz-Zuordnung zerstört Mobilität per Definition eine vorher etwa vorhandene räumliche Zuordnung. Welche Konzepte stehen hier für große Abdeckungsbereiche und zur Integration mit verkabelten Backbone-Netzen zur Verfügung?

Sprachdienste

Alle großen Marktforschungs-Institute sagen den VoIP Markt als unaufhaltsam voraus. Nach Dell'Oro waren bei Anlagen mit mehr als 100 Anschlüssen in 2005 schon 60 bis 70 Prozent der Lösungen VoIP-Lösungen. Allgemein wird das Überschreiten der Schwelle von 50 Prozent Marktanteil für die Jahre 2007 bis 2009 vorausgesagt (nicht nur Neukäufe sondern Gesamtmarkt). Die etablierten Carrier (AT&T, AOL, Telekom, BT) bieten zunehmend VoIP für Privatkunden zu attraktiven Preisen. Der Einzug von VoIP in Unternehmensnetze bedeutet:

- Betrieb einer neuen Klasse von Endgeräten (Handapparat, Bildschirmtelefon, WLAN Telefon, PDA, …)
- Betrieb neuer Server für TK-Handhabung und TK-Applikationen
- Betrieb neuer Gateways für non-IP und PSTN-Zugang
- Betrieb neuer Protokolle auf Basis IP (RTP, RTCP, RSTP, SRTP, SDP, SIP, SIMPLE, H.323, ABC, CorNet, DCS, MCDN, SCCP, …)

Stromversorgung

Sowohl für TK als auch für WLAN's besteht die Anforderung, Geräte mit niedriger Leistungsaufnahme über ihre Ethernet-Anschlüsse mit Strom zu versorgen, entweder um die Nutzung einer lokalen Stromversorgung zu vermeiden, oder weil die Geräte an Gebäudepunkten installiert werden, für die kein Stromanschluss in der erwünschten räumlichen Nähe verfügbar ist (z.B. WLAN Access Points). Hier ist seit mehreren Jahren der Standard IEEE 802.3af vorhanden, die „PoE"-Funktion wird mit ständig sinkenden Preisaufschlägen zunehmend einfach als Value Add in Layer-2/3 Switches verfügbar. Nur noch vereinzelte Hersteller verlangen für PoE-Modelle oder -Module im Vergleich zum non-PoE Gegenstück 20% oder 30% Aufpreis.

Lokalisierung

Insbesondere im Telefonumfeld ist das Absetzen von Notrufen eine wichtige bis unverzichtbare Funktion. Wie kann ein Benutzer, der mobil auf einem Firmengelände unterwegs ist, aufgefunden werden? Der Benutzer eines VoIP Telefons oder eines Laptops mit Webphone (Softphone als Web-Applet) kann sich in irgendeinem Bürogebäude, über irgendeinen Internet-Zugang eingeloggt haben. Wie lässt sich feststellen, von wo aus er gerade telefoniert? Auch für Störfälle in WLAN-Umgebungen ist die Lokalisierung der Störquelle vielfach Voraussetzung für die Fehlererkennung und -behebung.

Integration von Wireless und Wireline

In größeren vernetzten Umgebungen mit hohen Leistungsanforderungen ist die aktuelle wireless Technik hinsichtlich erzielbarer Datenrate und stabilem Durchsatz noch kein Ersatz für verkabelte Infrastruktur-Netze. Jedoch bietet sich Wireless LAN in mindestens zwei Bereichen als Ergänzungstechnik an. Zum einen können schlecht oder nicht verkabelbare Bereiche mit Funktechnik versorgt werden, zum anderen kann eine Flächenversorgung parallel zum verkabelten Netz für Mobilität sorgen. Hierdurch entsteht die Anforderung, beide Welten optimal zu integrieren, insbesondere für

- Nutzung der vorhandenen Verkabelung zur Anschaltung der WLAN Komponenten
- Übergang zwischen wireless und wireline
- Redundanz-Auslegung
- zentral gesteuerte Konfiguration
- zentralisiertes Management
- Interoperabilität verschiedener wireline und wireless Hersteller
- VLAN-Konzept und IP Subnetz-Konzept
- Layer-3 Roaming und Vermaschung über mehrere Hops
- QoS für Sprache oder andere kritische Dienste über WLAN

Sicherheit

Für den Betrieb von Wireless LAN's ist ein möglichst lückenloses Sicherheits-Konzept zwingend erforderlich, da Angriffe über die Luft als nicht begrenztes Medium leichter erfolgen können als über verkabelte Infrastrukturen. Hier liegen inzwischen mit IEEE 802.1X und IEEE 802.11i/WPA2 brauchbare Standards vor, die Sicherheits-Lösung ermöglichen, wenn auch mit hohem Aufwand. Gleichermaßen wird die Sicherheits-Lösung vielfach bei der Planung von TK-Lösungen über IP Netzwerke (VoIP) erneut diskutiert und auf den Prüfstand gestellt. Hinsichtlich Verschlüsselung, Zertifikat-Einsatz und IEEE 802.1X Unterstützung durch die IP-Telefone ist allerdings noch Raum für Verbesserungen gegeben.

Überwachung, Störfalldiagnose
Hersteller-Management-Systeme und unabhängige Monitoring-Lösungen integrieren die Media- und Signalisierungs-Protokolle etablierter VoIP Standards (H.323, SIP) und Hersteller (Alcatel, Cisco, Siemens, …). Vielfach ist jedoch noch kein integriertes Management von Daten- und TK-Netzkomponenten möglich, noch weniger steht ein integriertes Management von wireline und wireless Netzkomponenten zur Verfügung.

Resultierende Änderungen
Aus den Anforderungen ergeben sich Änderungen und Weiterentwicklungen in unterschiedlichen Netzbereichen. Zur Beschreibung dieser Änderungen greifen wir auf das LND-X5 Konzept mit Edge, Access, Concentrator, Core und Backend Bereichen (EACCB) für Design-Optimierung zurück, das im Insider Artikel „Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN„ vom Februar, März und Juni 2005.

Änderungen im Edge / Access Bereich:
- Einsatz und Betrieb neuer Endgerätetypen: Telefon, Headset, Handset, Bildschirmtelefon, PDA, Blackberry, WLAN Telefon, Dual Mode GSM / WLAN Telefon
- Integration von Wireless Technologien
- QoS für WLANs: proprietär, SpectraLink, WMM
- Migration zu Power via MDI (PoE)
- Lokalisierung von Benutzern / Endgeräten für Notruf, Fehlerdiagnose, Management-Statistiken (LLDP, LLDP-MED)
- Zugangskontrolle mittels Port Security, Policy, Sicherheits-Scan, „Gast-“ und „Quarantäne-Zugang“
- Automatische Zuweisung spezieller VLAN‘s beim Booten
- Konfiguration verschiedener wireless und wireline VLAN‘s für „Benutzergruppen-Trennung“

Änderungen im Concentrator Bereich:
- Schnellere Fehlerumschaltung: Standards (RST, OSPF, VRRP) versus proprietäre Verfahren (SMLT, GLBP, HSRPv2, EAPS, MRP, HIPERRing e.a.)
- Failover vs. Load Balancing (VRRP, GLBP)
- Steigende Verfügbarkeits-Anforderungen für Voice-Readiness
- Einsatz von Policies für Sicherheit und QoS bei kritischen Anwendungen (TK / Voice)
- Zentrale Integration und Steuerung von Mobilität durch WLAN-Switching, „Thin AP“ Konzepte

Änderungen im Core Bereich:
- Five-Nine-Verfügbarkeit
- Katastrophen-Absicherung durch geografisch getrennte Core-Bereiche
- Schnelle Fehlerumschaltung: Standards (RST, OSPF, VRRP) versus proprietäre Verfahren (SMLT, RSMLT, EAPS, MRP, HIPERRing e.a.)
- Zunehmend Preisverfall und Etablierung der 10 Gbit Ethernet Technik
- Zentrale Integration und Steuerung von Mobilität durch WLAN-Controller, „Thin AP“ Konzepte
- Durchschalten mehrerer bis vieler VLAN‘s für Mobilität / WLAN-Integration
- Einsatz von Policies für Sicherheit und QoS bei kritischen Anwendungen (TK / Voice)
- Einsatz zentral gesteuerter IDS / IPS Lösungen, Rückkopplung zu Netzmanagement und Policies
- Einrichtung von „Gast-“ und „Quarantäne-Zonen“
- Einsatz und Korrelation neuer Management / Monitoring Techniken (SMON, sFlow, LLDP MIB‘s)

Nachfolgend werden wir zuerst auf Neuerungen im wireless Umfeld, abschließend auf Neuerungen im wireline / Ethernet Umfeld eingehen.

2. Integration von wireless und wireline

2.1 Rasterkonzepte
Wegen der Installations-, Investitions- und Betriebs-Aufwände wurde bisher in vielen WLAN-Planungen mit teilweise recht aufwändigen Site Surveys versucht, die Anzahl der eingesetzten Access Points zu minimieren. Somit muss ein mobiler Benutzer je nach seinem Standort auch mit größeren Entfernungen zu einem Access Point (AP) leben. Hier sinkt jedoch der Durchsatz quadratisch zur Entfernung vom AP, wie Abbildung 2.1 verdeutlicht. Dasselbe gilt für Flächenkonzepte mit minimierter Überlappung. Der Gesamtdurchsatz ist niedriger als der maximal mögliche Durchsatz, da mit steigender AP-Dichte (bis hin zu einem Optimum) trotz Überlappung eine höhere Gesamtleistung erreichbar ist. Als eine mögliche Lösung hat sich

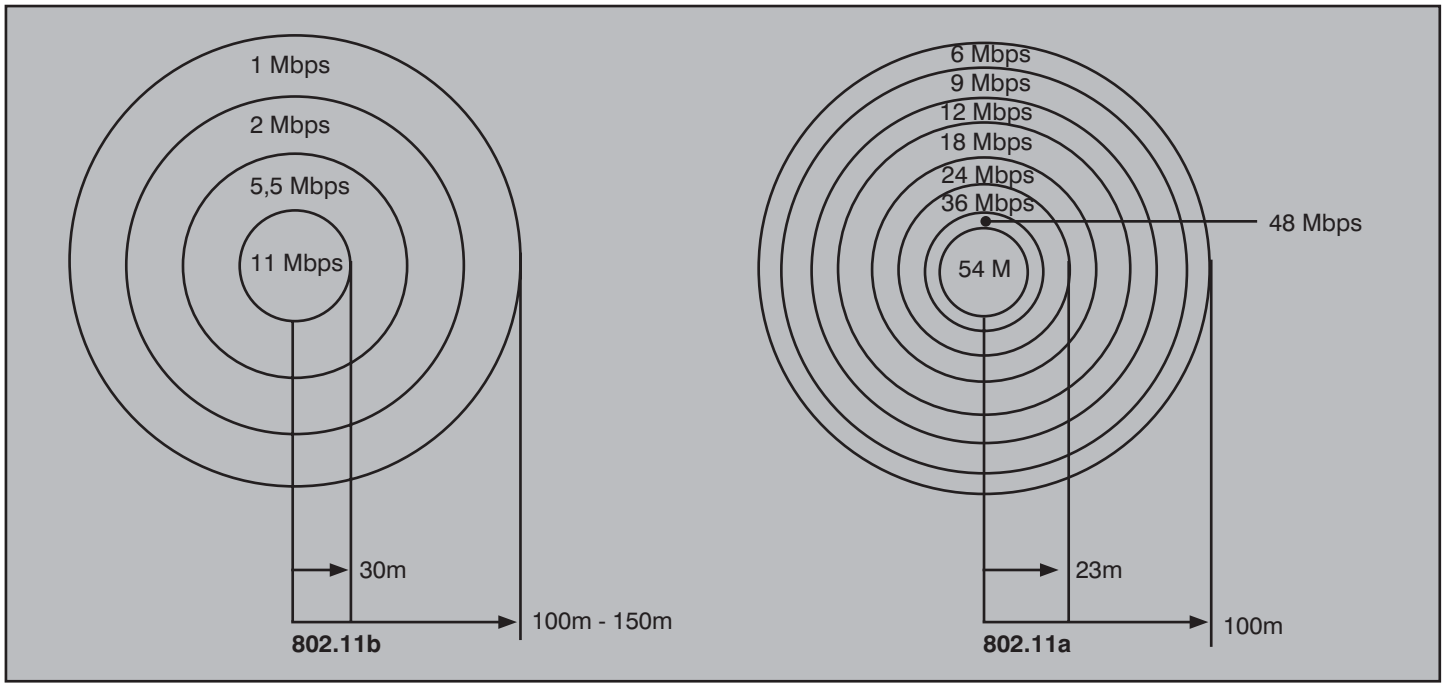


Abbildung 2.1: Einsatz von 10GbE-Ready Switchstacks

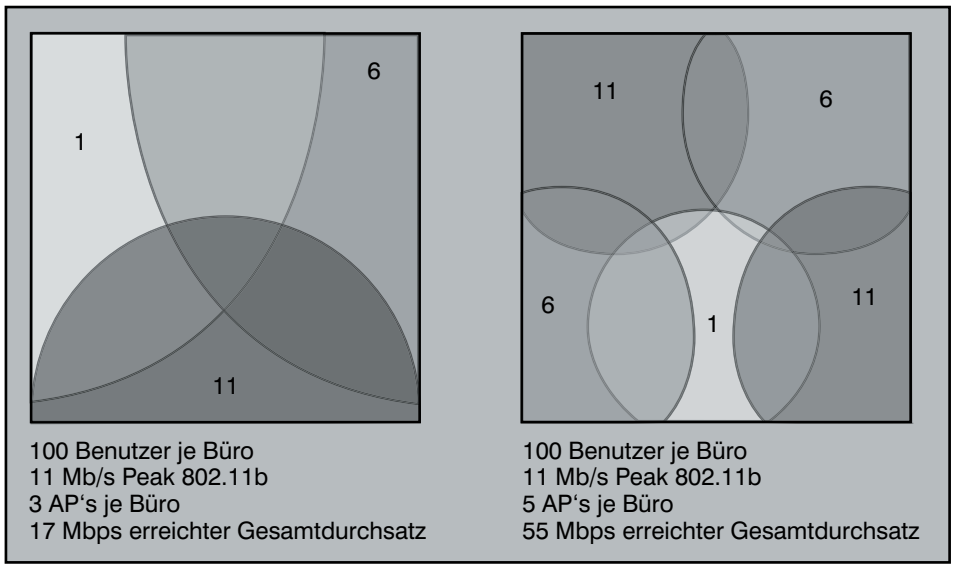


Abbildung 2.2: Gesamtdurchsatz bei unterschiedlicher AP-Dichte zur Flächenabdeckung

die dichtere Abdeckung mit Access Points als Gegenstück zur Überprovisionierung im verkabelten Bereich entwickelt. Im gezeigten Beispiel (siehe Abbildung 2.2) wurde derselbe Bürobereich einmal mit 3 Access Points und einmal mit 5 Access Points ausgerüstet. Trotz Überlappung ist der gemessene Gesamtdurchsatz bei 5 Access Points höher, da die maximale Entfernung zum nächsten Access Point an jedem möglichen Standort geringer ist als bei 3 eingesetzten Access Points. Im gezeigten Beispiel wurde eine Leistungssteigerung von 74% erreicht, gleichzeitig reduzierte sich das Delay um 91%.

Für eine maximale Reichweite müssen Access Points vielfach in ausreichender Höhe, also an der Decke oder im oberen Wandbereich montiert werden, da sich von hier aus die Funksignale am besten ausbreiten können. Dies führt zur Installation einer separaten Verkabelungs-Infrastruktur für Flächenkonzepte, denn wer hat in seiner liegenden Verkabelungs-Infrastruktur schon Kabel an die Decken geführt? Die Installation dieser „Parallel-Verkabelungsinfrastruktur" wird umso teurer, je größer die abzudeckende Fläche und je schwieriger der verkabelungstechnische Deckenzugang ist. Dies gilt nicht nur für die Erstinstallation sondern auch alle nachfolgenden Wartungsarbeiten. Die Kosten für einen Deckenanschluss können von mehreren 100 bis zu mehreren 1000 Euro reichen.

Soll die Stromversorgung mit PoE über den Ethernet-Anschluss erfolgen, so müssen entsprechende Power Hubs oder PoE Switches zum Einsatz kommen. Muss die

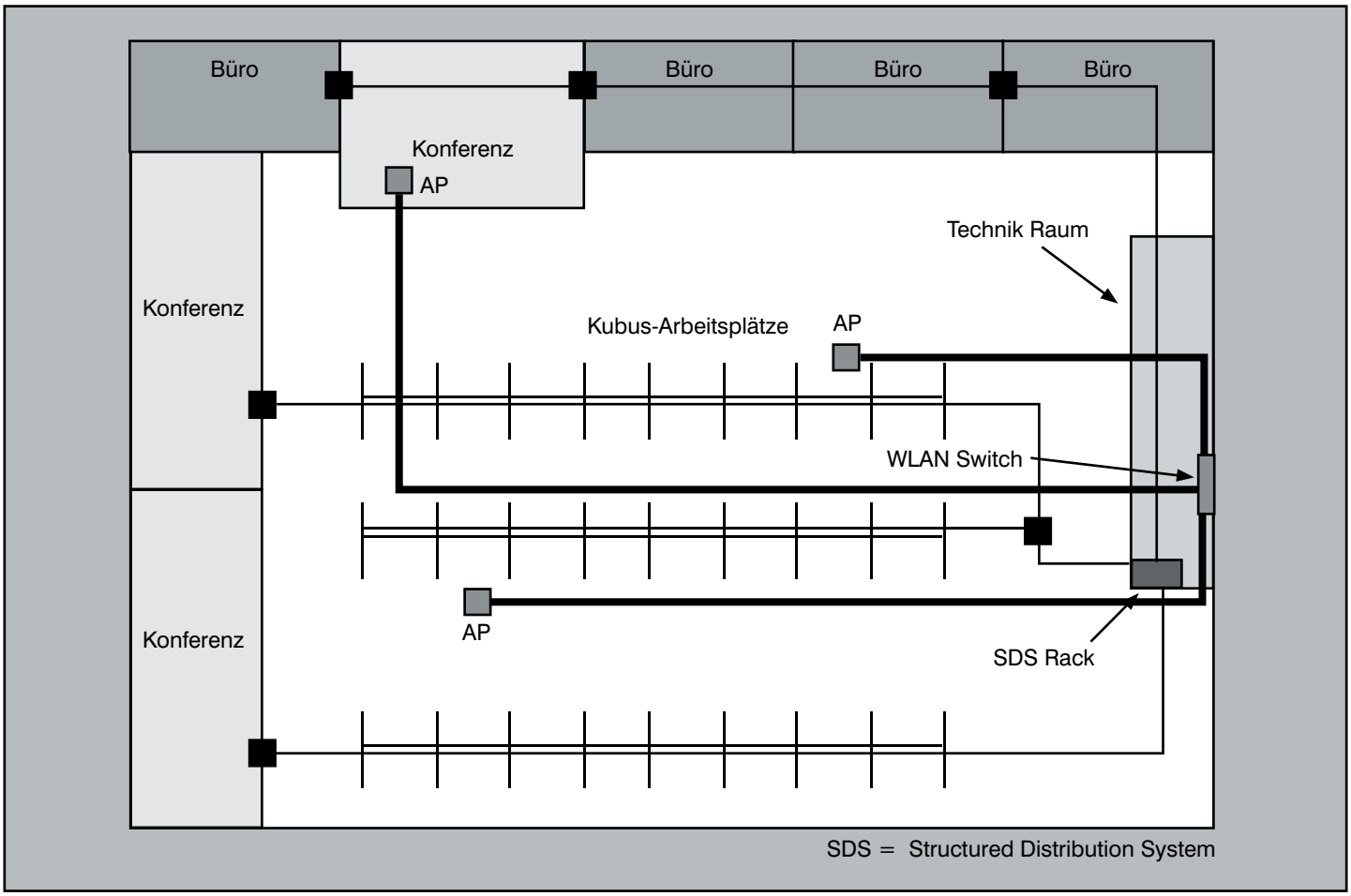


Abbildung 2.3: Separate Verkabelung und Minimierung der Anzahl Access Points

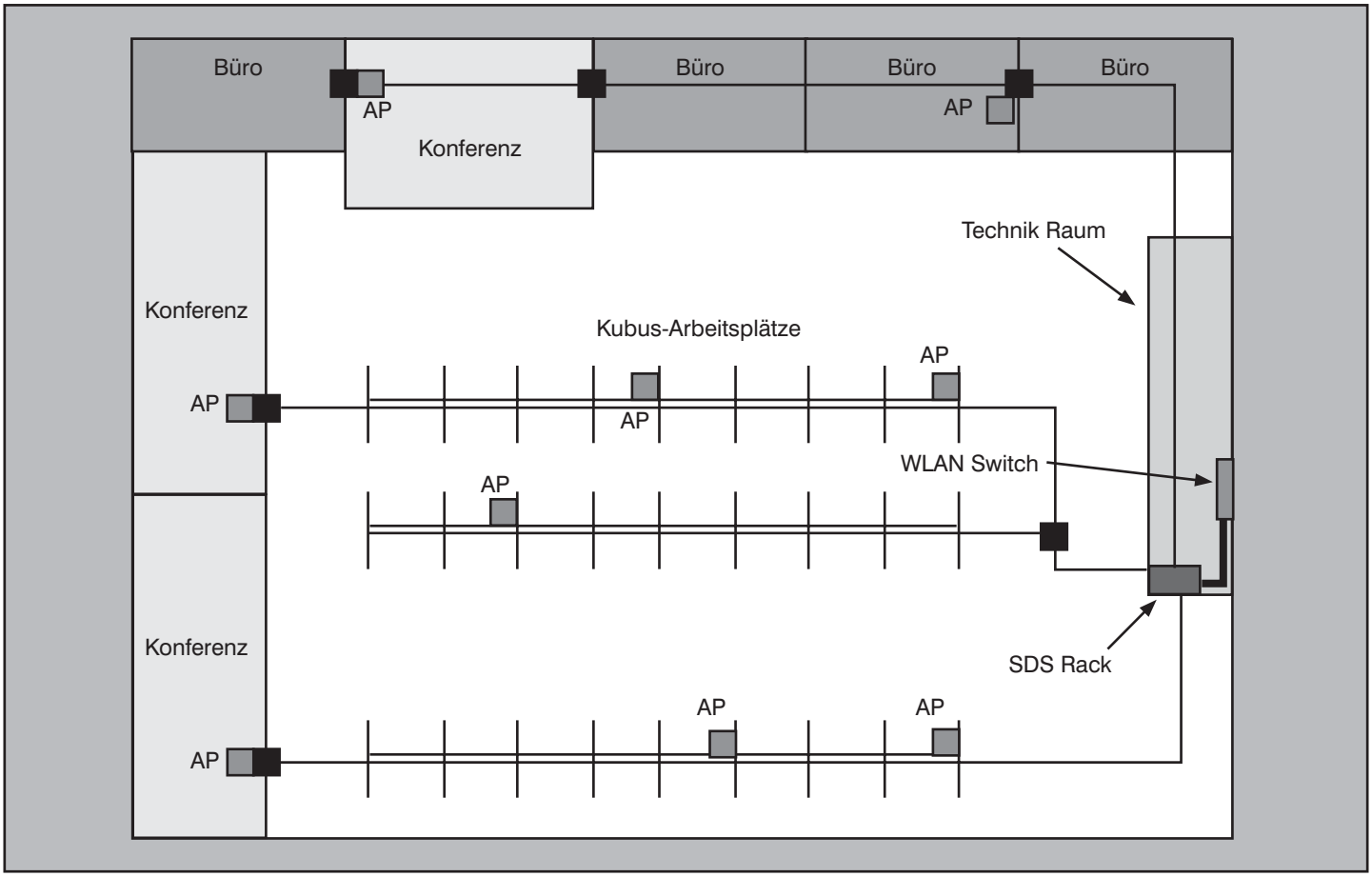


Abbildung 2.4: Ausnutzung der verlegten strukturierten Verkabelung zum Anschluss von Access Points

Stromversorgung des AP über den lokalen Stromkreis erfolgen, so befindet sich meistens auch keine Steckdose in Deckenhöhe, was die Installationskosten nochmals erhöht. Das Beispiel eines Großraumbüros in Abbildung 2.3 zeigt die separate Verkabelung für eine minimierte Anzahl von 3 Access Points, die mit Deckenmontage installiert wurden.

Wie sieht es dagegen mit der Nutzung der vorhandenen Verkabelung eines Gebäudes aus? Hier befinden sich die Ethernet Anschlussdosen oft in ca. 15 bis 30 cm Bodenhöhe und innnerhalb von Büroräumen. Wird ein Access Point hier angeschlossen, wird seine Reichweite geringer sein, für die erforderliche Flächendeckung wird eine höhere Anzahl AP's installiert. Eine solche dichtere Flächenbestückung wird als Rasterkonzept oder Gitterkonzept bezeichnet. Dies bedeutet, weniger Benutzer sind zum selben Zeitpunkt am selben Access Point assoziiert, derselbe Kanal kann öfter genutzt werden, Interferenzen werden geringer. Insbesondere zusammen mit einem zentralen Management, das eine RFSM Steuerung der Access Points zur optimalen Ausrichtung ihrer Sendeleistung unterstützt, ist hier keine allzu große Leistungseinbuße zu erwarten. Insgesamt bietet daher die Nutzung vorhandener Anschlüsse interessante Möglichkeiten, um den Gesamtdurchsatz zu erhöhen. Darüber hinaus können Rasterkonzepte den Aufwand für Site Surveys erkennbar reduzieren.

Allerdings ist hierfür eine zentralisierte WLAN Architektur erforderlich, bei der eine Management-Komponente alle beteiligten Access Points hinsichtlich Kanalzuweisung und Sendeleistung kontrollieren kann. Diese Architektur ermöglicht den Einsatz „weniger intelligenter" Access Points mit niedrigeren Stückkosten. Im Extremfall werden solche „Thin" Access Points so reduziert, dass sie wie reine Antennen arbeiten und nur die physikalische Übertragung (PHY) leisten. Die 802.11 MAC-Funktionalität ist in diesem

Merkmale von Rasterkonzepten

- Dichte und strukturierte AP-Packung für Flächenabdeckung
- Anbringung der AP's in nächster Nähe zu einer Wandanschlussdose
- Kleinere Zellgröße, daher geringere Kollisions- / Contention-Phänomene
- Erkennung und Lokalisierung von Interferenzquellen
- Vermeiden von Co-Channel Interferenz durch TPC (Transmit Power Control)
- Nutzung von PoE für den AP
- Software-programmierbare Access Points
- Management der AP's durch einen oder mehrere zentral positionierbare redundante Controller
- Dreidimensionale Adress-Hierarchie zur Lokalisierung von Rasterpunkten
- Wi-Fi Antennen agieren als „Zugangs-/Service-Punkt" (Rasterpunkt)
- Fokussierung der RF Signale auf einen kleinen Bereich
- Verteilen der RF-Dienste auf mehrere Raster AP's
  - Sicherheits-Funktionen
  - Lokalisierung, Tracking
  - Überwachung / Monitoring
  - Fehlerdiagnose
  - Kalibrierung

Fall auf eine zentral positionierte Komponente ausgelagert, wie später näher erläutert wird.

Leider sind die Kosten pro Access Point trotzdem nicht so niedrig, dass die dichtere Bestückung d.h. höhere Anzahl zu demselben Preis wie die weniger dichte Stückzahl bei Deckenmontage führt. Werden jedoch alle Montagekosten inklusive zusätzlicher „WLAN-Verkabelung“ und höhere Betriebsaufwände eingerechnet, können sich durchaus Kostenvorteile ergeben. Das Beispiel in Abbildung 2.4 zeigt dasselbe Großraumbüro wie zuvor, jetzt mit 9 installierten Access Points, die an die vorhandene strukturierte Verkabelung angeschlossen sind.

Als Erweiterung unterstützen einige Hersteller Client-Treiber, die nicht am aktuellen AP assoziiert bleiben, bis das Signal so schwach ist, dass ein Wechsel zum nächsten AP zwingend erfolgen muss, sondern schon vorher nach bestimmten Kriterien wie Signalstärke, freier Kanal o.ä. den „jeweils günstigsten“ AP auswählen.

2.2 WLAN Redundanzkonzepte

Sobald WLAN Technologie in einem Unternehmen flächendeckend und als teilweise Ablösung von verkabelten Netzen eingesetzt wird, entsteht die Anforderung nach einer redundanten Auslegung. Eine detailliertere Beschreibung der möglicher Redundanz-Lösungen wurde in dem Insider Artikel vom März 2005 „Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN - Teil 2“ dargestellt. An dieser Stelle erfolgt daher nur eine Zusammenfassung der verschiedenen Möglichkeiten:

- Überlappende Installation von Funkzellen, Überprovisionierung von Access Points
- Ausrichtung der Access Points und Regelung ihrer Sendeleistung (TPC) durch zentrale Steuerung über einen WLAN Switch oder WLAN Controller; dies erfordert Kommunikation zwischen Access Point und WLAN Client, d.h. Steuerung des Client durch den AP.
- Zukünftig wird der Standard IEEE 802.11v mittels zentraler Konfiguration und Management der WLAN Clients die Voraussetzung für ein besseres Handover zwischen zwei AP‘s schaffen, der IETF Standard CAPWAP könnte eine für Multivendor-Kommunikation zwischen Controller und Access Point ermöglichen.
- Der Einsatz von Rapid Spanning Tree wird aktuell von Access Points nicht unterstützt. Der Einsatz von klassischem Spanning Tree wird nur in wenigen Fällen unterstützt, da nur wenige Access Points redundante Ethernet Anschlüsse haben (z.B. Trapeze, Aruba). Spanning Tree über die Funk Schnittstelle und mehrere Radioteile scheint sich derzeit nicht zu etablieren.
- Mesh WLAN Konzepte bilden proprietäre fehlertolerante, über Funkverbindungen vermaschte Netzwerke, ähnlich dynamisch gerouteten verkabelten Netzwerken.

Auf die Themen „zentrale Steuerung von Access Points“ und „Mesh Networks“ wird im weiteren detaillierter eingegangen.

3. Aufteilung der Intelligenz: „WLAN Switching“ und WLAN Controller

Die ersten Generationen von Access Points implementierten die volle IEEE 802.11 WLAN-Funktionalität und wurden im Regelfall als flache Layer-2 Peer-to-Peer Infrastruktur implementiert (siehe Abbildung 3.1). Jeder Access Point bildete eine separate RF-Domäne und musste separat gemanagt werden. Eine zentrale Instanz, welche die Übersicht über das gesamte WLAN Netzwerk hat, gab es nicht.

Der Einsatz dieser „Fat Access Points“ oder Autonomer Access Points bedingt einige Limitierungen

- Management: separates Management jedes Access Points
- Sicherheit: keine Erkennung netzweiter Angriffe; Diebstahl von Access Points
- Mobilität: keine Korrelation von Interferenzen, keine Prognose für Benutzeraktivitäten; kein subnetzübergreifendes Layer-3 Roaming
- Authentifizierung: EAP Requests werden in RADIUS enkapsuliert und ohne jedes Offload an den AAA Server gesendet; dieser muss folglich alle verwendeten EAP Methoden (PEAP, LEAP, EAP-TLS, TTLS, …) ebenso wie Master Kay Generierung unterstützen
- Kosten: höherer Preis je Access Point im Vergleich zu AP‘s mit reduziertem Funktionsumfang

Zur Beseitigung dieser Limitierungen wurden Konzepte mit zentraler Steuerung der Access Points entwickelt, die sich unter dem Namen WLAN Switching oder WLAN Controlling etablieren. Der Begriff WLAN Switch ist sehr missverständlich, da hier keinesfalls die dedizierte Leistungszuordnung wie beim LAN Switching gemeint

ist! WLAN Controller ist eigentlich die treffendere Beschreibung. Beide Begriffe werden relativ schwammig im Markt benutzt. Hersteller solcher Lösungen sind z.B. Airespace (Cisco), Aruba, Chantry (Siemens), Extreme, Nortel, Symbol, Trapeze, Vernier und Weru. Die verfügbaren Konzepte unterscheiden sich im Umfang der zentralisierten Funktionalität und auch in der Architektur der zentralen Kontroll-Instanz.

Wie startet und integriert sich ein Thin Access Point, der so reduziert wurde, dass er keine Anfangskonfiguration hat? Entweder hat er einen statischen Eintrag mit der Adresse des Controllers (z.B. Siemens/ Chantry) oder findet über ein spezielles Discovery Protokoll den nächsten WLAN Controller; letzteres ist natürlich die deutlich betriebsfreundlichere Variante. Mittels Beacon oder Probe Request erfolgt die Assoziation an dem gefundenen Access Point.

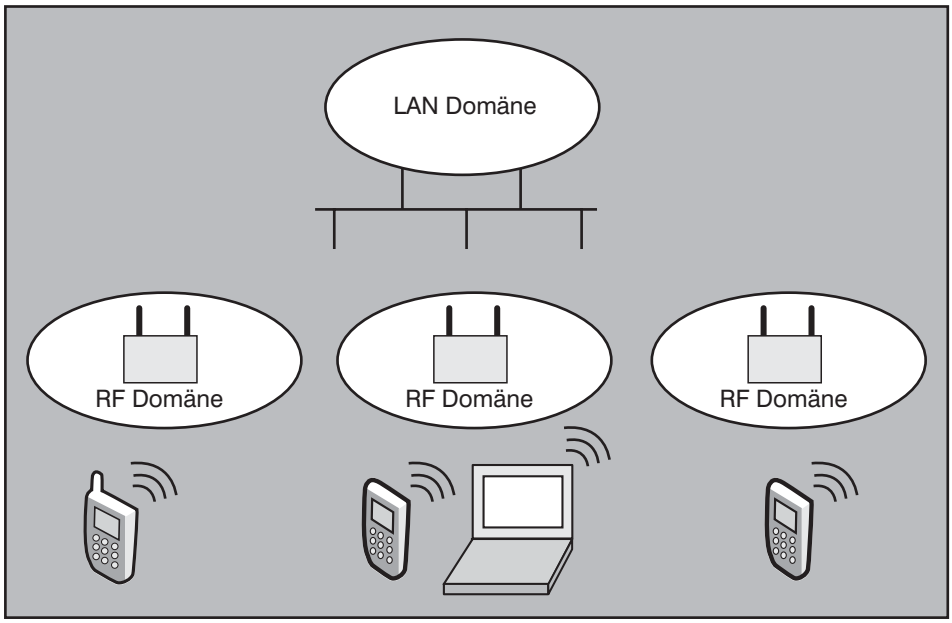


Abbildung 3.1: Peer-to-Peer WLAN mit Fat Access PointsPoints

Produkt-Beispiele

Es gibt Hersteller, die sowohl WLAN Switches als auch Controller Produkte anbieten, bei genauerem Hinsehen können Controller als Weiterentwicklung der WLAN Switches bezeichnet werden. Trapeze z.B. bietet kleine WLAN Switches (Mobility Exchange) für 2, 12 oder 40 Access Points (Mobility Point) und einen Controller an (Lizenzen für 40, 80 oder 120 Access Points). Insgesamt können bis zu 32 WLAN Switches und etwa 3000 Access Points im Verbund betrieben werden.

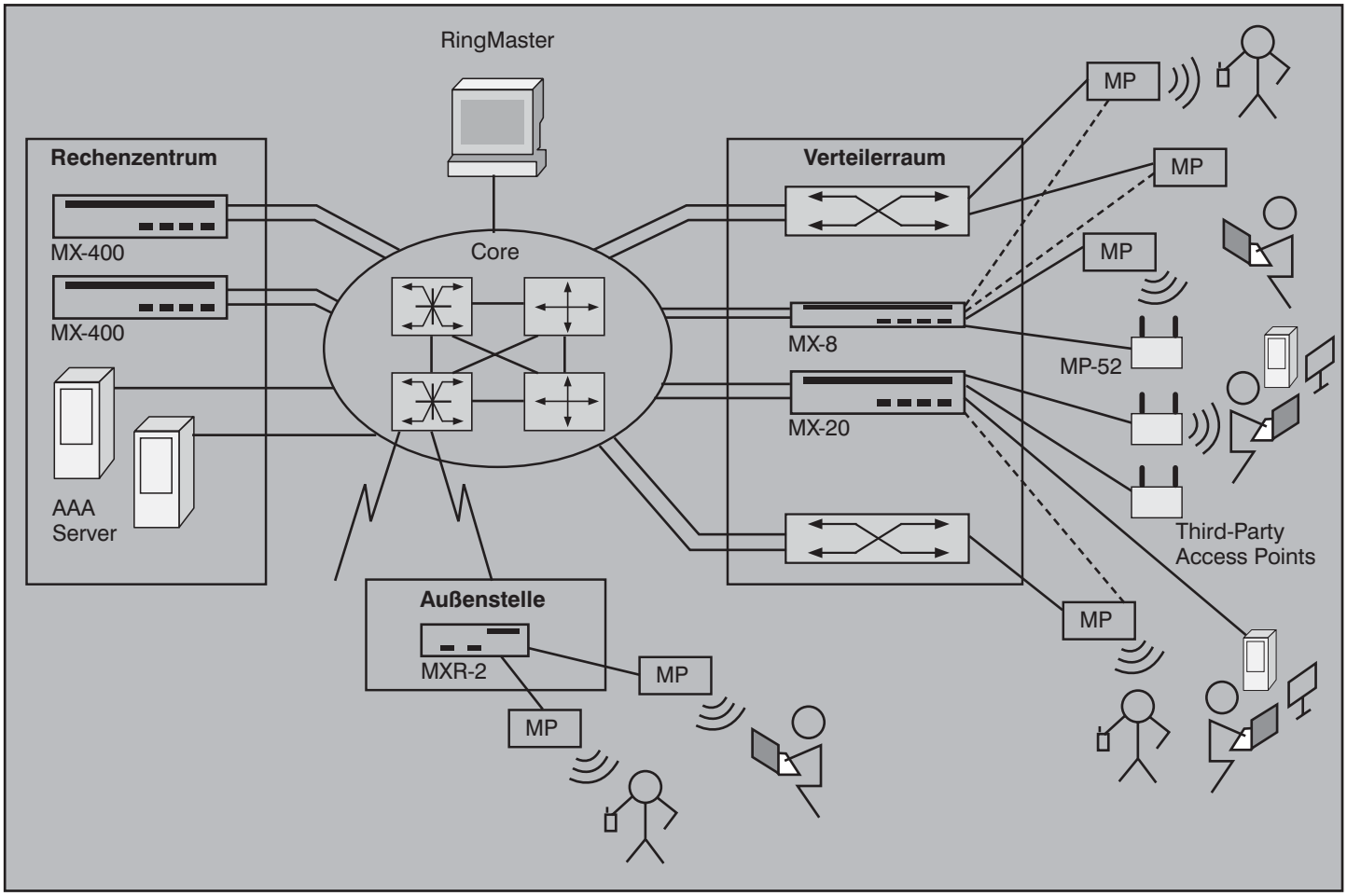


Abbildung 3.2: WLAN Domäne über mehrere Standorte hinweg mit zentraler Steuerung durch WLAN Switches und WLAN Controller

Auf den WLAN Switches und dem Controller läuft dieselbe Software (MSS Mobility System Software), WLAN Switches und WLAN Controller können zusammen in einem gemeinsamen WLAN Verbund mit N+1 Redundanz betrieben werden. Das Beispiel in Abbildung 3.2 zeigt herstellereigene und 3rd Party Access Points, die sowohl an WLAN Switches als auch an normale Ethernet Switches angeschaltet sind. In einem zentralen Verteiler werden zwei redundante Controller betrieben. Die Anzahl bedienbarer Access Points ergibt sich aus der Summe der maximalen Access Points, die mit den WLAN Switches / den Controllern bedienbar sind.

Siemens (Chantry) hat eine rein Controllerbasierte Lösung und gibt eine maximale Anzahl von 200 Access Points je Controller an, hier ist eine 1+1 Redundanz erforderlich. Es gibt keine offizielle obere Grenze für die maximale Anzahl Access Points, die in einem Verbund von Controllern betreibbar sind (größte bisherige Installation nach Herstelleraussagen: 700 AP‘s).

Cisco (Airespace) kann mehrere Controller in einem Cluster betreiben, die dann nicht LWAPP, sondern ein eigenes Protokoll zur Controller-Controller Kommunikation verwenden der Hersteller gibt eine Obergrenze von 24 Controllern und maximal 3000 Access Points an, wobei die tatsächlich erreichbare Größe von den jeweiligen Mobility Groups abhängt.

Funktionen von WLAN Switches und WLAN Controllern
Typische Funktionen solcher zentralisierten Konzepte lassen sich in verschiedene Bereiche aufteilen:

- Management
  - Gemeinsame IP Adresse für mehrere AP‘s
  - RF Management und Tuning (dynamische Kanalzuweisung, TPC, Load Balancing (Airespace, Aruba))
  - Lokalisierung (Airespace)
  - Echtzeit-Statistiken (Aruba)
  - Zentrale grafische Konfiguration für VLAN‘s, QoS, Policies, Sicherheit (Airespace, Aruba)
  - Klassifizierung für QoS (Trapeze)
- Sicherheit
  - Authentifizierung (Aruba, Trapeze)
  - Verschlüsselung (Aruba, Trapeze teilweise)
  - Netzweite Sicherheitsregeln (Airespace) und Filter (Trapeze)
  - Erkennen von DoS-Angriffen, Erkennen und Ausgrenzen von Rogue AP‘s (Airespace)
  - Schutz vor Diebstahl, da der AP alleine nicht arbeitsfähig ist
- Mobilität
  - Handover, GSM-ähnlicher Fast Handoff (Airespace)
  - Echtzeit Unterstützung für Voice, Fast Roaming (Airespace)
  - Durchschalten von VLAN‘s bei Roaming, damit kein VLAN-Wechsel erfolgen muss (Airespace, Siemens/Chantry, Trapeze e.a.)
  - VPN Terminierung (Aruba)
- Aufbau von Mobilitäts-Domänen
  - Verbund mehrerer WLAN Switches (Trapeze)
  - Informationsabgleich / Roaming mittels Synchronisierung über Switch-Switch Protokoll (Trapeze)
- Multivendor-Unterstützung
  - Einbindung von Multivendor AP‘s: Generische Enkapsulierung mit Interoperabilität mit Layer-2 oder Layer-3 Kopplung; Achtung: Die 3rd Party Einbindung hat meistens nicht denselben Funktionsumfang wie die Einbindung der herstellereigenen AP‘s! (Airespace, Trapeze)

WLAN Switches

Als WLAN Switch werden eher Lösungen bezeichnet, bei denen die zentrale Kontrolle als Software oder als Zusatzmodul in einem Layer-2 oder Layer-3 Ethernet-Switch implementiert ist. Die Access Points werden teilweise direkt an den Ethernet Switch angeschaltet, teilweise ist zur Anschaltung eine beliebige Layer-2 Verbindung zwischen Access Point und WLAN Switch erlaubt. Im Regelfall können WLAN Switches eine geringere Anzahl AP‘s handhaben als Controllerlösungen. Teilweise sind die Access Points funktional bis hin zum reinen „Funk-Ethernet-Konverter“ reduziert.

Der Einsatz von WLAN Switches beinhaltet weiterhin einige Beschränkungen: Eeine Mobilitäts-Domäne kann auf einen einzelnen Switch beschränkt sein, oder es gibt eine Limitierung der maximalen Anzahl von WLAN Switches, die in einer gemeinsamen Mobilitäts-Domäne betreibbar sind. Der Einsatz spezieller Ethernet Switches (vom selben Hersteller wie die Access Points), die dann als WLAN Switch arbeiten, erzwingt den Betrieb eines weiteren Switchtyps im Ethernet Netzwerk, der sich hinsichtlich Konfiguration, Management, allgemeiner Ethernet-Switch-Funktionalität und Ersatzteilhaltung von den anderen Switches unterscheidet. Das proprietäre Protokoll, das zwischen WLAN Switch und Access Points zum Einsatz kommt, führt zur Herstellerabhängigkeit, da Access Points und WLAN Switches zwingend oder aber mindestens zur Erreichung des vollen Funktionsumfangs vom selben Hersteller sein müssen.

WLAN Controller

Die zuvor genannten Einschränkungen von WLAN Switches führten in konkurrierenden Entwicklungsansätzen oder in der Weiterentwicklung zu WLAN Controllern. Controller Lösungen verwenden als zentrale Kontrollinstanz eine Appliance, vielfach auf Basis Linux (oder Unix), die im Regelfall zentral und im Netzwerk positioniert ist. Eine vernünftige Controller-Lösung lässt sich dabei hot standby redundant auslegen, so dass bei Ausfall eines Controllers eine schnelle Fehlerumschaltung erfolgt, die einen Sessionverlust vermeidet.

Vorteile der Controller Lösung liegen insbesondere in der höheren Skalierbarkeit, in der Unabhängigkeit der Access Points von den eingesetzten Ethernet Switches und darin, dass zwischen Access Point und Controller auch eine Layer-3 Verbindung vorliegen kann (die Verbindung ist nicht mehr zwingend auf Layer-2 beschränkt). Eine Layer-3 Verbindung erlaubt die Erweiterung des Konzepts auf mehrere Standorte, teilweise werden am remote Standort „Mini-“Controller eingesetzt, die es ermöglichen, dass die dort installierten (wenigen) Access Points auch arbeitsfähig bleiben, wenn der zentrale Controller oder die WAN-Verbindung ausfällt.

Anforderungen an WLAN Controller

An den WLAN Controller als zentrale Komponente des gesamten WLAN-Netzwerks sind einige Anforderungen zu stellen: Er muss hinsichtlich Speicherausbau und CPU-Leistung ausreichend skalieren, d.h. die geplante Anzahl von AP‘s handhaben können oder auf ein Cluster-Konzept erweiterbar sein. Er muss eine hohe Anzahl

von VLAN's und Tunneln bedienen können, in einigen Fällen bis hin zu einem separaten Tunnel je Benutzer (!). Um die Verfügbarkeitsanforderungen an größere WLAN Installationen zu erfüllen, muss der Controller redundant im hot standby betreibbar sein. Arbeitet er gleichzeitig als RADIUS Server, so muss er alle Authentifizierungs-Vorgänge ohne Leistungseinbuße in der Datenweiterleitung bedienen können, gegebenenfalls auch die aller non-WLAN Clients (!).

Zur Übersicht verschiedener Ansätze mit Fat Access Points, Thin Access Points, WLAN Switches und WLAN Controllern dient die Vergleichstabelle in Abbildung 3.3.

VLAN's und Roaming

Ein zentrales Element von WLAN Switching und Controller Lösungen ist die Sicherstellung minimaler Handoff- und Roaming-Zeiten, auch wenn der WLAN Client sich über die Grenzen seines lokalen IP Subnetzes hinaus bewegt. Diese Funktion wird oft als Fast Roaming bezeichnet. Um eine erneute Authentifizierung und

Konzept	**Fat Access Point**		**Thin Access Point / WLAN Switch**		**Thin Access Point / WLAN Controller**	
	Implementierung	Auswirkung	Implementierung	Auswirkung	Implementierung	Auswirkung
Konfiguration	manuell oder Download per Management	limitierte Skalierbarkeit	automatisches Lernen vom WLAN Switch	gute Skalierbarkeit	zentraler Download vom WLAN Controller	gute Skalierbarkeit
Implementierung	komplex, Site Survey erforderlich	hoher Aufwand von Kosten und Ressourcen	einfacher aufgrund Rasterkonzepten und Management-Tools	Einsparung von Kosten und Ressourcen	einfacher aufgrund Rasterkonzepten und Management-Tools	Einsparung von Kosten und Ressourcen
Direkter Zugang	Konsole	Sicherheitsrisiko	nein	Schutz gegen Kompromittierung	nein	Schutz gegen Kompromittierung
Redundanz	meistens nur 1 Ethernet Port	eineschränkte Verfügbarkeit	teilweise 2 Ethernet Ports	gute Verfügbarkeit	nicht unterstützt	AP ist Single Point of Failure
802.1X Authentifizierung	Authenticator im AP, aber Request Weiterleitung an AAA Server	Gesamtlast der Authentifizierung auf AAA Server	WLAN Switch oder AAA Server als Authenticator	skalierbar auf mehrere Komponenten verteilt	WLAN Controller oder AAA Server als Authenticator	belastet zentralen Server
Verschlüsselung	**teilweise, Software**	langsamer	Hardware	entlastet AAA Server	Verschlüsselung über WLAN Controller oder AAA Server	belastet zentralen Server
Mehrere Benutzergruppen	eine SSID je Gruppe erforderlich, limitierte Anzahl von Gruppen	ggf. Änderung der L3-Struktur, große L2 Domänen	Vermaschung von WLAN Switches mit begrenzter Anzahl SSID's und Tunneln	gute Skalierbarkeit, mittlere Komplexität	selbe SSID für verschiedene Gruppen / VLANs mit Tunnel-Konzepten möglich	ggf. hohe Anzahl von Tunneln, mittlere Skalierbarkeit, erhöhte Komplexität
Benötigte VLAN's, Tunnel	mittel	mittlerer Aufwand	niedrig	niedriger Aufwand	hoch	hoher Aufwand
Roaming	ggf. neue Routing Protokolle auf AP und Router (IP-in-IP Tunnel je Roaming User)	erhöhter Installationsaufwand, limitierte Skalierbarkeit	Mobilitäts-Domänen über mehrere Switches hinweg	mittlerer Overhead, gute Skalierbarkeit	komplett über WLAN Controller	hohe Belastung des zentralen Servers, mittlere Skalierbarkeit
Rogue AP Erkennung	eingeschränkt	mittlerer Schutz	ja	guter Schutz	meistens nein	kein Schutz
Access Control Listen	nein oder eingeschränkt	manuelle Konfiguration	je nach Hersteller unterstützt oder nicht	zentral konfigurierbar analog zu vorhandenen ACL	nein	ACL nicht wirksam im WLAN Bereich
Zentrale Logdatei	nein	limitierte Korrelation von Meldungen	ja	gute Korrelation von Meldungen	ja	gute Korrelation von Meldungen
QoS / CoS	ja	QoS / Cos implementierbar	Queues im AP, Klassifizierung im WLAN Switch	QoS / Cos implementierbar	Klassifizierung im WLAN Controller	QoS / Cos im Wireline Bereich, nicht im WLAN Bereich
VPN Server für Sicherheit	teilweise integriert	kein Single Login, nicht für Voice geeignet (langsames Roaming)	nicht benötigt	transparent für externe VPN Server	nicht benötigt	erhöhte Komplexität bei parallelen VPN Tunneln und WLAN Tunneln
DHCP Server	teilweise integriert	Seiteneffekte mit vorhandenen DHCP Servern	nicht benötigt	transparent für externe DHCP Server	nicht benötigt	transparent für externe DHCP Server

Abbildung 3.3: Vergleich verschiedener Access Point Konzepte

neue IP-Konfiguration mittels DHCP zu vermeiden (beides bedingt zu hohe Antwortzeiten für Fast Roaming), wird in vorhandenen Lösungen das VLAN / IP Subnetz beibehalten, dem der WLAN Client beim Login in das WLAN und Assoziierung an den ersten Access Point zugeordnet wurde. Das gesamte WLAN Netzwerk, innerhalb dessen Roaming erfolgt, wird als flaches Overlay Netzwerk über das darunterliegende Transportnetz betrieben. Ist die Anzahl der WLAN Clients so groß, dass eine einzelne gemeinsame flache Layer-2 Domäne nicht mehr ausreicht, so werden mehrere Overlay Netze eingerichtet, die sich je nach Bewegung der ihnen zugeordneten Clients auch überlagern können. In jedem Fall merkt der Client nicht, dass er durch mehrere („physikalische“) Subnetze hindurchwandert, er bleibt immer in „seinem“ flachen Layer-2 VLAN.

Wie wird dies erreicht? Durch eine ganz alte Technik: Tunneling! Zwischen Access Point und WLAN Controller oder WLAN Switch wird für den Tunnel die MAC-Adresse des jeweiligen Access Points und die MAC-Adresse des Controllers / WLAN Switches als MAC-Quell- und –Zieladresse der getunnelten Frames eingesetzt. Sollten sich also mehrere 1000 Benutzer heftig von einem Ort zum anderen bewegen, kann dies schlimmstenfalls zur Bildung von mehreren 1000 Tunneln führen. Unterschiedliche Herstellerlösungen verwenden entweder Layer-2 (Ethernet in IP) oder Layer-3 Tunnel (IP in IP). Ein wichtiger Punkt bei der Beurteilung einer zentralisierten WLAN Lösung ist daher die Frage: Wie werden Tunnel aufgebaut und wie viele Tunnel entstehen? Welche Antwortzeiten entstehen bei einer hohen Anzahl von Tunneln und gleichzeitig abzuarbeitenden Authentifizierungs-Requests? Werden Tunnel von Benutzern / WLAN Clients, die zuvor im selben VLAN waren, an einem Access Point wieder einem gemeinsamen VLAN und Tunnel zugeordnet? Im gezeigten Beispiel der Abb. 3.4 sind die WLAN Clients drei verschiedenen VLAN‘s / IP Subnetzen zugeordnet, Subnetz 1 und 2 für Daten und Subnetz 3 für IP Telefonie. Die zugeordneten VLAN‘s sind unabhängig von den räumlich zugeordneten IP Subnetzen der verkabelten Infrastruktur. Die WLAN Clients Otto und Hugo haben beim Login dasselbe VLAN / IP Subnetz erhalten. Beide haben sich inzwischen in andere Netzbereiche bewegt, ihr VLAN wird in diese Bereiche durchgetunnelt. Bewegt sich nun Otto an den Access Point, an dem Hugo assoziiert ist, so wird der Tunneling Overhead entscheidend reduziert, wenn Otto und Hugo über denselben Tunnel mit dem Rest der Welt kommunizieren. Der Overhead steigt dagegen in hohem Maße, wenn für jeden Benutzer bei jedem subnetzübergreifenden Roaming ein neuer Tunnel eingerichtet wird.

Sollen WLAN-Domänen untereinander kommunizieren, die durch verschiedene WLAN Switches oder Controller bedient werden und somit verschiedene Mobilitäts-Domänen bilden, richten die beteiligten WLAN Controller Tunnel zueinander ein. In diesem Fall läuft sämtlicher domänenübergreifender Datenverkehr zweier WLAN Domänen über beide beteiligte WLAN Controller. Gleiches gilt für den Overhead zur Client-Steuerung, falls eine solche vom

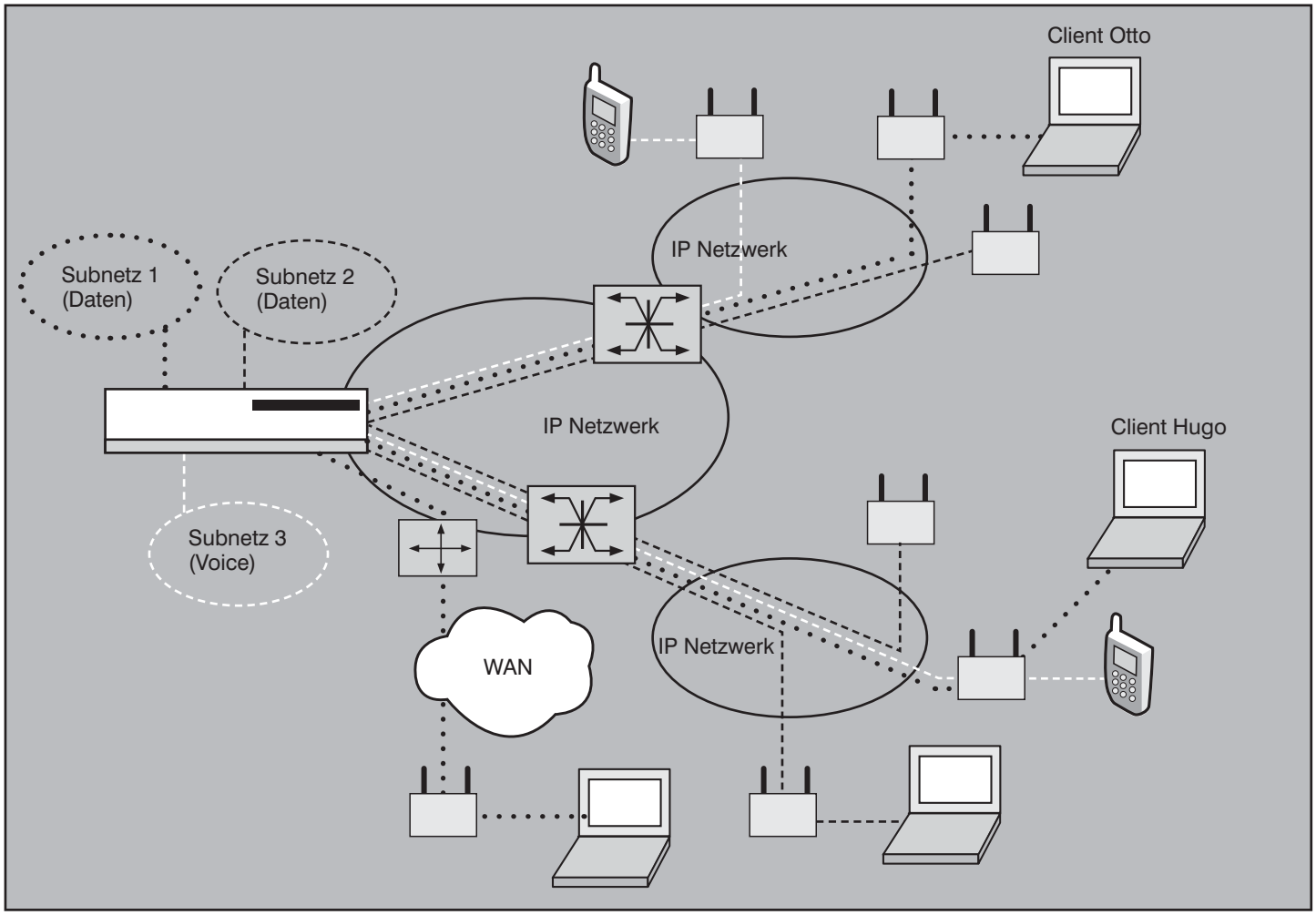


Abbildung 3.4: Tunnelbildung beim Roaming von WLAN Clients

Controller aus erfolgt und ein Client sich von seiner Ursprungs-Domäne in eine andere Domäne bewegt hat.

4. IETF Standardisierung: CAPWAP

Da die Hersteller mehr und mehr zentralisierte WLAN Konzepte vermarkten, versucht nun eine IETF Arbeitsgruppe „Control and Provisioning of Wireless Access Points (CAPWAP), eine standardisierte Lösung zu spezifizieren, in der sich Access Points und WLAN Controller herstellerübergreifend kombinieren und betreiben lassen. Im ersten Schritt wurde auf der Basis von 15 Herstellerlösungen eine Spezifikation der grundsätzlichen Funktionen sowie eine Kategorisierung der verschiedenen auf dem Markt verfügbaren Architekturen erarbeitet, da unterschiedliche Architekturen die einzelnen Funktionen unterschiedlich auf Controller und Access Points verteilen. Die Verabschiedung eines RFC's ist jedoch realistischerweise nicht von Ende 2006 zu erwarten.

Als Begrifflichkeit wurde für den Access Point die Bezeichnung WTP (Wireless Termination Point) für die Funkschnittstelle zum Client eingeführt, die Bezeichnung AC (Access Controller) für die zentrale Kontrollinstanz.

Die Architekturen werden unterteilt in
- Autonomes WLAN
- Zentralisiertes WLAN
  - Local MAC
  - Split MAC
  - Remote MAC
- Verteiltes, vermaschtes WLAN

Das **Autonome WLAN** (siehe Abbildung 4.1) entspricht der bekannten „Fat Access Point" Architektur, für die ja ebenfalls ein Bedarf nach zentralisiertem Management und zentralisierter Konfiguration besteht. Hier ist der WTP ein standalone Gerät, das die IEEE 802.11 Distribution Dienste, Integration Dienste und die Portalfunktion leistet.

Das **Zentralisierte WLAN** (siehe Abbildung 4.2) besteht aus einem Access Controller AC (dieses Architektur-Element könnte aus zwei redundanten Komponenten bestehen), der die Control Plane, d.h. Management Kontrolle und Konfiguration der WTP's implementiert. Zusätzlich kann (nicht: muss) der AC eine Aggregierung der Data Plane durchführen (Tunneling für Layer-3 Roaming). Die WTP's implementieren die Data Plane, d.h. senden und empfangen die Nutzdaten-Frames. Wireless Termination Points sind über eine – aktuell verkabelte – Anbindungs-Infrastruktur mit dem Access Controller ver-

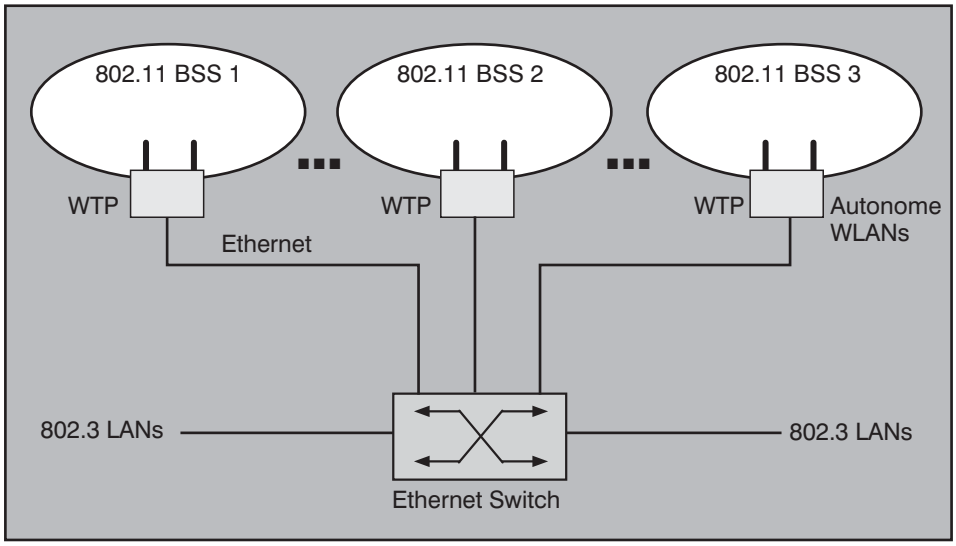


Abbildung 4.1: CAPWAP Architekturen, Autonomes WLAN

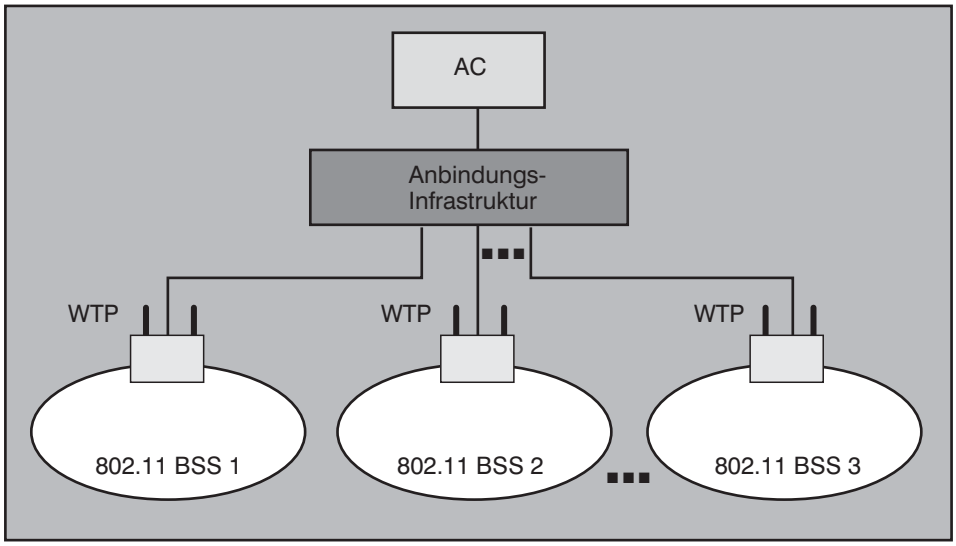


Abbildung 4.2: CAPWAP Architekturen, Zentralisiertes WLAN

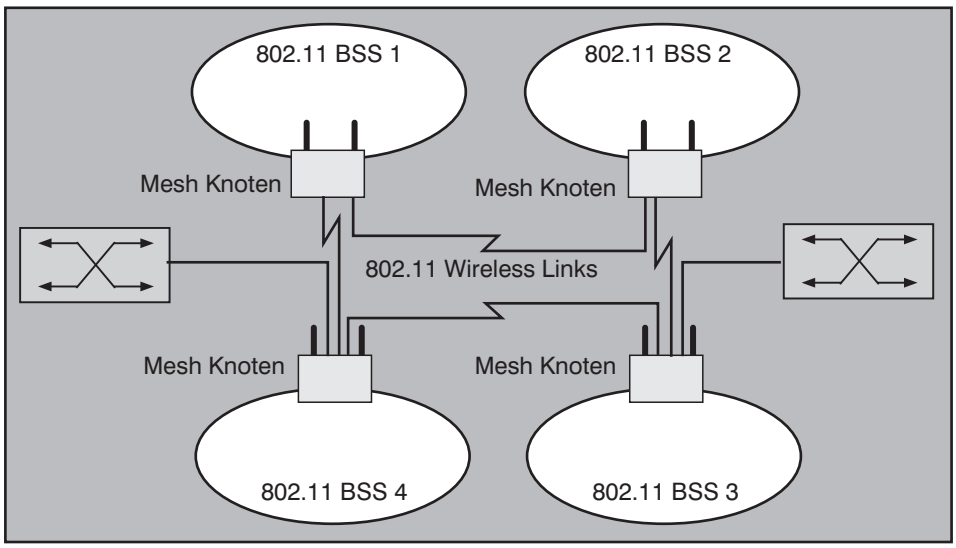


Abbildung 4.3: CAPWAP Architekturen, Vermaschtes / Verteiltes WLAN

bunden. Je nach Architektur kann diese Anbindungs-Infrastruktur auf Layer-2 Verbindungen eingeschränkt sein oder Layer-3 Verbindungen zulassen.

Das **Vermaschte / Verteilte WLAN** besteht nicht aus WTP's und AC sondern aus gleichberechtigten Knoten, die mittels Funkverbindung vermascht sind. Ein oder mehrere Knoten realisieren die Verbindung zur verkabelten Infrastruktur (siehe Abbildung 4.3). Ein Knoten kann Access Point und Relay zu benachbarten Knoten sein, er kann auch als reiner Relay Knoten ohne Client Access agieren. Jeder Knoten hält Informationen über den Zustand seiner Nachbarknoten vor. Bei Anschalten eines neuen Knotens führt dieser eine Selbstkonfiguration durch. Bei Ausfall einer Funkverbindung oder eines Knotens erfolgt Fehlerumschaltung auf die verbleibenden Knoten ähnlich dem dynamischen Routing in verkabelten Netzen. Das Thema Mesh WLAN's wird im zweiten Teil dieses Beitrags weiter detailliert.

Der Arbeits-Fokus der CAPWAP Gruppe liegt aktuell auf einer Lösung für Zentralisierte WLAN's bei gleichzeitiger Berücksichtigung Autonomer WLANs. Vermaschte / Verteilte WLAN's wurden nur am Rande in die Kategorisierung aufgenommen. Die verfügbaren vermaschten Lösungen bleiben vermutlich proprietär, bis der IEEE 802.11s Standard für vermaschte WLANs vorliegt.

CAPWAP Aufteilung der benötigten Funktionen

CAPWAP unterteilt die benötigten Funktionen in CAPWAP Funktionen (Kontrolle) und 802.11 WLAN Funktionen (Daten)

CAPWAP Funktionen sind
- RF Monitoring
- RF Konfiguration
- WTP Konfiguration
- WTP Firmware
- Datenbank für Stations-Status
- Wechselseitige AC èç WTP Authentifizierung

802.11 WLAN Funktionen sind
- Stations-Dienste
- Distributions-Dienste: Verteilung von MAC Frames innerhalb des DS auf Basis der Assoziierungen
- Integrations-Dienste: Verbindung zwischen 802.11 DS und non-802.11 LAN

Die 802.11 MAC-Funktionen werden bei den Split MAC Architekturen in Echtzeit- und non-Echtzeit-Dienste aufgeteilt. Der WTP leistet die Echtzeit-Dienste, die non-Echtzeit-Dienste werden auf den AC ausgelagert. Allerdings stellt die CAPWAP-

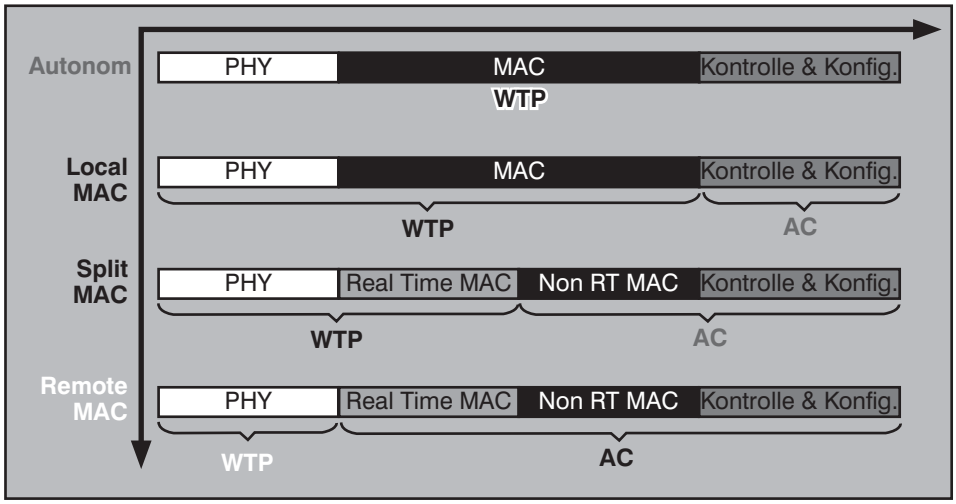


Abbildung 4.4: Funktionsaufteilung bei Local MAC, Split MAC und Remote MAC

Auffassung von Echtzeit und non-Echtzeit einen gemeinsamen Nenner dar und wird nicht von allen Herstellern exakt so geteilt. In manchen Herstellerkonzepten unterscheidet sich die Echtzeit/non-Echtzeit Unterteilung daher vom aktuellen CAPWAP Diskussionsstand.

CAPWAP sieht folgende Zuordnung der IEEE 802.11 WLAN Dienste:
- MAC-Funktionen (Echtzeit) wie
  - Synchronisierung
  - Retransmission
  - MAC Control Frames
  - Senderaten-Anpassung
  - Beacon Generierung (Echtzeit)
  - Probe Senden / Beantworten (Echtzeit)
  - Paketpufferung bei Power Mgmt./Power Save (non-Echtzeit)
  - Fragmentierung / Defragmentierung (non-Echtzeit)
  - Assoziieren / Disassoziieren / Reassoziieren (non-Echtzeit)
  - Integrations-Dienst (non-Echtzeit)
  - WME 802.11e (non-Echtzeit)
    - Klassifizierung
    - Scheduling, Queueing
  - Authentifizierung, Vertraulichkeit (non-Echtzeit)
    - 802.1X / EAP

- Schlüsselmanagement, Verschlüsselung / Entschlüsselung

Im Kern ergeben sich einige wesentliche Unterschiede zwischen Local MAC, Split MAC und Remote MAC, die hier zusammengefasst werden (siehe auch Abbildung 4.4).

Local MAC: Der Wireless Termination Point ist autonom arbeitsfähig. Management und die Handhabung von Policies sind jedoch auf den Access Controller ausgelagert, um die eingangs beschriebenen Kosten-, Skalierbarkeits- und Betriebsvorteile zu erreichen. Die IEEE 802.11 Funktionen laufen vollständig auf dem WTP, er terminiert alle MAC-Frames.

Split MAC: Der Wireless Termination Point ist nicht mehr autonom arbeitsfähig. Er terminiert die Wireless Infrastruktur auf der physikalischen Ebene, terminiert die zeitkritischen (Echtzeit-) MAC Funktionen und handhabt das RF Management. Der AC ist außer für Management und Policies auch für Konfiguration, non-Echtzeit MAC Funktionen (Integration Service), Quality of Service (QoS), Lastverteilung und ACL's (Access Control Listen) zuständig. Für den Einsatz von Split MAC Lösungen ist zu beachten, dass diese bei sehr zeitkritischen Anwendungen wie Produktion oder anderen Echtzeit-Umgebungen Probleme machen können, wenn die erforderlichen Antwortzeit-Restriktionen von den zum zentralen Access Controller ausgelagerten MAC-Funktionen nicht eingehalten werden. Dieser Punkt wird von der Spezifikation nicht berücksichtigt, da die Anwendungs-Ebene für CAPWAP „out of scope" ist.

Remote MAC: Es erfolgt eine Trennung der IEEE 802.11 Funktionen nach MAC und PHY (Layer 2 und Layer 1). Der Wireless Termination Point arbeitet quasi rein als Antenne und leitet die empfangenen Bits physikalisch an den Access Controller weiter. Dieser leistet alle 802.11 MAC Dienste, zusätzlich RF-Management, Kanalauswahl, Netzmonitoring / Management, Policies, ACL's, Sicherheitsfunktionen und QoS. Bei Remote MAC Konzepten ist klar, dass die Anbindungs-Infrastruktur nur eine sehr geringe Ausdehnung und Kaskadierung haben kann, um die für 802.11 erforderlichen Zeitrestriktionen einzuhalten. Wir geben dieser Variante daher keine allzu großen Marktchancen.

CAPWAP Protokolle

Die Kommunikation zwischen Wireless Termination Point und Access Controller verläuft in mehreren aufeinander folgenden Sequenzen. Beim Start führen WTP und AC folgende Schritte durch:

1. **Discovery:** WTP's suchen ihren zugehörigen AC. Die Suche kann statisch konfiguriert oder dynamisch ablaufen. Bei statischer Konfiguration muss in jedem WTP ein Eintrag hinterlegt sein, wer der AC ist bzw. wie er gefunden wird. Im Fall einer dynamischen Discovery ist ein WTP ← → AC Protokoll erforderlich.

2. **Authentifizierung:** Zuerst authentifiziert sich der WTP gegenüber seinem AC. Eine wechselseitige Authentifizierung ist nicht immer unterstützt, z.B. bei wenn auf WTP Seite noch gar keine Konfiguration und somit auch kein Authentifizierungs-Protokoll zur Verfügung steht! Dies kann naturgemäß im Sicherheitsumfeld zu Problemen führen.

3. **WTP Assoziierung:** Der WTP registriert sich an dem AC, den er gefunden hat, für Management und Konfiguration

4. **Firmware Download:** Der Firmware Download zum WTP erfolgt entweder via „WTP Pull" oder via „AC Push". Der Download kann (nicht: muss) geschützt sein, z.B. mit einer digitalen Signatur.

5. **Control Channel Einrichtung:** Für Datentransfer und Management baut der WTP einen Layer-3 IP Tunnel oder einen Layer-2 Ethernet Tunnel (Enkapsulierung) zum AC auf.

6. **Konfigurations-Download:** Nach Aufbau des Control Channel kann der AC dem WTP Konfigurations-Parameter mitteilen.

Die zuvor beschriebenen und im weiteren Betrieb (Überwachung, Management) erforderlichen Kommunikations-Sequenzen verwenden ein eigenes Protokoll. Derzeit stehen in der CAPWAP Arbeitsgruppe verschiedene Protokollvarianten zur Debatte, die von unterschiedlichen Herstellern vorerst als konkurrierende Drafts eingereicht wurden und teilweise in den Produkten dieser Hersteller schon (als Vorversion) implementiert sind:

- LWAPP - Lightweight Access Point Protocol (Airespace/Cisco, DoCoMo, Legra)
- CTP - CAPWAP Tunneling Protocol (Chantry/Siemens)
- SLAPP - Secure Light Access Protocol (Airespace/Cisco, Aruba)
- WiCop - Wireless LAN Control Protocol (Panasonic)

Der älteste Draft und der mit den meisten Überarbeitungen ist das Leight Weight Ac-

cess Point Protocol LWAPP, das von Airespace entwickelt wurde und folglich in den Airespace/Cisco Komponenten zum Einsatz kommt.
Eine erste Evaluierung der eingereichten Protokollvorschläge durch CAPWAP-Teams, welche eine faire Beurteilung sicherstellen sollten, liegt seit August 2005 vor. Die Auswertungs-Übersicht zeigt Abbildung 4.5.

Offene Punkte bei CAPWAP

Sind WLAN Switches, WLAN Controller oder nach CAPWAP standardisierte WTP und AC Komponenten ein endgültiges Lösungskonzept? Oder sind sie ein Workaround mit den typischen Schwächen zentralistischer Architekturen und getunnelter Datenübertragung? Die Standardisierung von Management und Konfiguration wäre zumindest einmalig in der Netzwerk-Geschichte der letzten 15 Jahre. Immerhin gibt es im Endgeräte-Bereich funktionierende Beispiele für die Vereinheitlichung ähnlicher Funktionen. Aktuell besteht jedoch ein nicht zu unterschätzendes Risiko, dass zentralisierte Architekturen und insbesondere die aktuellen WLAN Tunneling Konzepte wieder verschwinden, sobald ordentliche vermaschte WLAN-Lösungen auf den Markt kommen.

Eine weitere Frage ist die, welches Protokoll sich letztlich durchsetzen wird. LWAPP? SALPP? CTP? WiCop? Ein Kompromiss zwischen LWAPP und SLAPP? Oder ähnlich wie die EAP-Lösung: SLAPP als Überbau und darunter eine Auswahlmöglichkeit für LWAPP, CTP oder WiCop? Der gemeine Kölner würde an dieser Stelle sagen: „Mer weiß et nit“.

Einige Funktionen fehlen auch bei CAPWAP: Für Lokalisierung und Fast Roaming existieren bisher nur proprietäre Ansätze (für Lokalisierung sind die Markt-Entwicklungen hinsichtlich IEEE 802.1AB LLDP und LLDP-MED zu beachten).

Falls ein Access Controller sich als RADIUS Server bekannt gibt, läuft sämtlicher Authentifizierungs-Verkehr über diesen Access Controller, auch alle Requests von verkabelten Clients (!). Selbst wenn der AC hierfür genügend leistungsfähig ist, kann die WLAN Infrastruktur einen Engpass darstellen.

Last but not least stellt sich die strategische Frage: Was wird aus den WLAN Switch und WLAN Controller Herstellern, wenn die etablierten Ethernet Switch Hersteller CAPWAP in ihre Switches oder auf Appliance Servern implementieren?

CAPWAP Evaluierung					
		LWAPP	SLAPP	CTP	WiCoP
1	Logical Groups	C	C	C	C
2	Traffic Separation	C	C	P	P
3	STA Transparency	C	C	C	C
4	Config Consistency	C	C	C	C
5	Firmware Trigger	P	P	P	C
6	Monitor System	C	C	P	C
7	Resource Control	C	p	P	P
8	Protocol Security	C	C	F	F
9	System Security	C	C	F	F
10	802.11i Consideration	C	C	F	P
11	Interoperability	C	C	C	C
12	Protocol Specifications	C	P	P	P
13	Vendor Independence	C	C	C	C
14	Vendor Flexibility	C	C	C	C
15	NAT Traversal	C	C	C	C
Optionen					
1	Multiple Authentication	C	C	C	C
2	Future Wireless	C	C	C	C
3	New IEEE Requirements	C	C	C	C
4	Interconnection (IPv6)	C	C	C	C
5	Access Control	C	C	C	C

C = Compliant P = Partial Compliance F = Failure to Comply

Abbildung 4.5: Evaluierung der aktuell vorgeschlagenen CAPWAP Protokolle

Fortsetzung folgt!

Abkürzungen

AAA	Authentication, Authorization and Accounting
ABC	Alcatel Business Communication
AC	Access Controller
ACL	Access Control List(e)
AP	Access Point
AOL	America Online
AT&T	American Telephone & Telegraph Corporation
BSS	Basic Service Set
BT	British Telecom
CAPWAP	Control and Provisioning of Wireless
CorNet	Corporate Network (Siemens, ISDN)
CTPDCS	Distributed Communication System
DoS	Denial of Service
DS	Distribution System
EACCB	Edge, Access, Concentrator, Core, Backend
EAP	Extensible Authentication Protocol
EAPS	Ethernet Automatic Protection Switching
GLBP	Gateway Load Balancing Protocol
GSM	Global System for Mobile Communication
HIPERRing	High Performance Ring (Siemenst)
HSRP	Hot Standby Routing Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LB	Load Balancing
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP for Media Endpoint Devices
LND	Layered Network Design
LWAPP	Light Weight Access Point Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network

	(Stadtnetz)
MCDN	Meridian Customer Defined Network (Nortel)
MDI	Media Dependent Interface
MP	Mobility Point (Trapeze)
MRP	Multiservice Route Processor
MSS	Mobility System Software
MX	Mobility eXchange (Trapeze)
OSPF	Open Shortest Path First
PAN	Personal Area Network
PDA	Personal Digital Assistant
PHY	Physical Layer
PoE	Power over Ethernet
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAN	Regional Area Network
RF	Radio Frequency
RFSM	Radio Frequency Spectrum Management
RSMLT	Routed Split Multi-Link Trunking
RTP	Remote Power Control
RTCP	Real Time Control Protocol
RST	Rapid Spanning Tree
RSTP	Rapid Spanning Tree Protocol
SA	Scheduled Access
SCCP	Skinny Client Control Protocol
SDP	Session Description Protocol
sFlow	Switch Flow
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SLAPP	Secure Light Access Point Protocol
SMLT	Split Multi-Link Trunking
SMON	Remote Network Monitoring MIB Extensions for Switched Networks (Switch MONitoring)
SRTP	Secure RTP
TCP	Transmission Control Protocol
TK	Telekommunikation
TPC	Transmit Power Control
VLAN	Virtuelles LAN
VPN	Virtual private Network
VoIP	Voice over IP
VoFi	Voice over Wi-Fi
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WiCop	Wireless LAN Control Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WTP	Wireless Termination Point

Links

<aruba>
www.cisco.com
www.hp.com
www.nortel.com
www.siemens.com (vormals Chantry)
<trapeze>
www.tropos.com
<vernier>
<weru networks>
www.ieee.org/11
www.ieee.org/16
www.wimaxforum.org
www.wi-mesh.org

Liteatur

Farpoint Group: Rethinking the Access Point: Dense Deployments for Wireless LAN; August 2004

CCNE

ComConsult Certified Network Engineer

Lokale Netze
06.02. - 10.02.06 in Aachen
03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

Internetworking
06.03. - 10.03.06 in Aachen
08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP
13.02. - 17.02.06 in Bonn
15.05. - 19.05.06 in Stuttgart
25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand
20.02. - 24.02.06 in Aachen
29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
20.03. - 24.03.06 in Aachen
08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
30.01. - 03.02.06 in Aachen
24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung
06.02. - 10.02.06 in Köln
15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
20.03. - 22.03.06 in Bad Neuenahr
19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
03.04. - 07.04.06 in Aachen
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)

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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line 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