Dr. Suppan International Institute

Der Netzwerk Insider

September 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

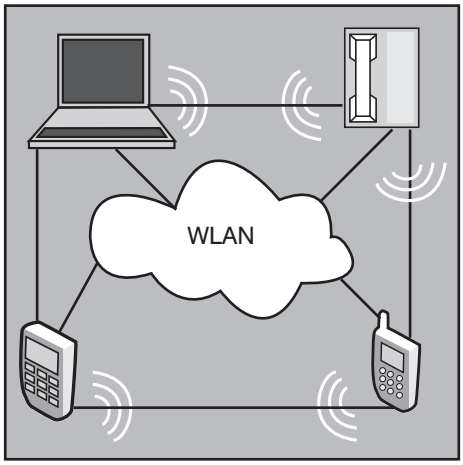
Schwerpunktthema

Rahmenbedingungen und Kriterien für einen zukunfts-orientierten WLAN-Einsatz

von Dr. Jürgen Suppan

Mit der Verabschiedung des IEEE 802.11i-Sicherheits-Standards haben Wireless-Netzwerke ihre Kinderkrankheiten endgültig hinter sich gelassen und sind eine ernstzunehmende Konkurrenz für kabelgebundene Netzwerke geworden.

Tatsächlich haben sie sich aus einer unsicheren Technologie zur sichersten heute verfügbaren Netzwerk-Technologie entwickelt. Gerade im Bereich der Spezialanwendungen von der Medizintechnik über den Produktionsbereich bis zu Transport und Warenlogistik wird dies den Einsatz von WLAN-Technik weiter beschleunigen. Mit der von IEEE 802.11i geforderten Sicherheits-Infrastruktur für Unternehmen werden auch die Auflagen zur Übertragung von Personendaten des Bundesdatenschutzgesetzes erfüllt (der Radius-Server muss dabei loggen). Gleichzeitig werden sich die nutzbaren Datenraten in den nächsten Jahren bis in den Gigabit-Bereich hinein erhöhen. Der Wechsel in die neuen Datenraten kann sanft erfolgen, da eine Planung und Umsetzung eines WLAN in einer Weise möglich ist, die eine einfache Migration in neue Datenraten mit geringem Aufwand gestattet.



weiter auf Seite 17

Zweitthema

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

von Dr.-Ing. Joachim Wetzlar

Open-Source ist in aller Munde - die lang ersehnte Befreiung von der Übermacht der Hersteller. Leider erkauft man sie sich häufig mit hohen Betriebskosten und Inkompatibilität. Nicht so bei der Protokollanalyse!

Im folgenden Artikel stelle ich Ihnen DAS Open-Source-Produkt zur Protokollanalyse vor und gebe eine kleine Starthilfe für seinen erfolgreichen Einsatz.

Haben Sie sich auch immer schon gefragt, warum Protokollanalyse so kompliziert ist? Zum einen ist der Grund dafür in der komplexen Materie an sich zu suchen: Damit zwei Computer über ein Datennetz miteinander kommunizieren können, ist eine nicht unerhebliche Zahl unterschiedlicher Protokolle vonnöten, angefangen bei den „physikalischen“ Protokollen der Schicht 1 - wie beispielsweise die Trellis-Kodierung bei Gigabit Ethernet - bis hin zum weiten Feld der Anwendungsspezifischen Protokolle der Schicht 7 - am eindrucksvollsten repräsentiert durch die „Server Message Blocks“ der Microsoft-Welt.

weiter auf Seite 8

Top-Event

Wireless LAN Forum 2004

auf Seite 5

Zum Geleit

Kampf um den neuen WLAN-Standard

auf Seite 2

Report des Monats

Wireless LAN Evaluierung

auf Seite 14

Zum Geleit

Kampf um den neuen WLAN-Standard

Am 12. August wurde die nächste Runde im Kampf um die Wireless-Zukunft eingeläutet. An diesem Tag mussten alle Vorschläge (Proposals) zur Bearbeitung für den IEEE 802.11n-Standard eingereicht worden sein. Zwei Interessengruppen kämpfen dabei um die Zukunft im Wireless-Markt. Der Hersteller Belkin geht sogar so weit, ein Vorstandard-11n-Produkt für Oktober 2004 anzukündigen.

Worum geht es dabei? Wie unsere Analysen, die wir zum Netzwerk-Redesign-Forum als Exklusiv-Studie veröffentlicht haben, zeigen, beinhaltet die Wireless-Technologie noch erheblichen Spielraum für Verbesserungen, insbesondere im Bereich der Erhöhung der Datenrate.

Das Ergebnis unserer Studie, die von Dr. Kauffels erarbeitet wurde, zeigte ein Übertragungsratenpotenzial im Gigabit-Bereich auf. Die aktuellen Arbeiten am IEEE 802.11n-Standard stellen in diesem Zusammenhang einen Kompromiss dar, in dem sie versuchen, Mehrleistung ohne Steigerung der Kosten für Client-Adapter und Access Points zu erreichen.

So sind die Ziele von IEEE 802.11n angesichts der erheblichen Potenziale, die noch in der WLAN-Technik stecken, schon fast bescheiden:

- Minimalziel: 100 Mbit/s real nutzbarer Durchsatz nach Abzug des Overheads
- Maximaldurchsatz: 540 Mbit/s inklusiv Overhead, real voraussichtlich um die 350 bis 400 Mbit/s
- Keine Erhöhung der Kosten für Access Points und Client-Adapter
- Erhöhung der Reichweite um den Faktor 4

Im Augenblick bevorzugen die am Standard beteiligten Firmen die so genannte MIMO-Technologie, eine Mehrwegtechnologie, bei der ein Sender im selben Kanal aber auf verschiedenen Wegen mit separaten Radioteilen sendet und der Empfänger entsprechend viele Radioteile für den Empfang benötigt.

Das ist letztlich eine positive Nutzung der auch bei „normalen“ WLANs auftretenden

Multipath-Effekte, die allerdings nur unter besonderen Voraussetzungen an die Vorkodierung funktioniert. Die ersten Produkte werden mit 2 Sendern und Empfängern arbeiten, der Standard wird voraussichtlich bis zu 4 beinhalten.

Streit gibt es um die Frequenzbreite eines Übertragungskanals. Die eine Interessengruppe mit Airo, Broadcom und TI bevorzugt 20 MHz-Kanäle, die andere um Agere, Atheros, Intel und Sony 40 MHz. Alle diese Überlegungen beziehen sich grundsätzlich auf den 5 GHz-Bereich.

Aus diesem Grund wird von den Vertretern des neuen Standards auch vollmundig die Kompatibilität zu 11b und 11g verkündet, was in der Realität bedeutet, dass der Kunde eine separate Lösung für diesen Bereich benötigt (die Access-Points werden wahrscheinlich wie jetzt auch einfach den Parallelbetrieb in einem Gerät integrieren).

Unklar ist zum jetzigen Zeitpunkt, wie die Interoperabilität mit 11a insbesondere bei der 40 MHz-Variante aussieht.

Angesichts dieser Entwicklung, die den 5 GHz-Bereich klar als den zukünftig führenden Frequenzbereich unterstreicht, ist die zögernde Umsetzung des 802.11a-Standards durch die Hersteller schon fast ein Skandal (man könnte auch hart sagen: Investitionsbetrug am Kunden).

Zwar wird 11a angeboten, aber vielfach halbherzig, indem nur eine 30 mW-Variante angeboten wird. Man verweist auf die RegTP und auf ETSI, die ja für die 200mW-Varianten Auflagen erhoben haben (DFS und TPC). Da diese Auflagen aber längst von fast allen Produkten erfüllt werden, stellt sich umso mehr die Frage, was die Hersteller eigentlich davon abhält, massiv in den 5 GHz-Bereich einzusteigen. Über die Antwort kann natürlich nur spekuliert werden.

Meine persönliche Sichtweise ist klar. Wichtige und im Markt starke Hersteller haben noch kein Interesse daran, dass Wireless ein wirklicher Ersatz für Kabelgebundene Netzwerke wird. Immerhin macht der Umsatz mit Workgroup-Switches zwischen einem Drittel und der Hälfte des Gesamtumsatzes dieser Hersteller aus. Die Strategie ist dann auch folgerichtig und aus meiner Sicht durchaus nachvollziehbar: Wireless-Technik wird solange forciert solange sie nicht Infrastruktur-fähig in dem Sinne ist, dass sie dem Kabel Konkurrenz macht.

Und so viel haben unsere bisherigen Analysen eindeutig gezeigt: IEEE 802.11b und IEEE 802.11g sind kein genereller Ersatz für ein Kabel. Dabei ist nicht die Übertragungsrate entscheidend. Der Hauptaspekt, der gegen den Einsatz von 11g als flächiger Infrastruktur spricht, ist die Reduzierung auf 3 überschneidungsfreie Kanäle. In Kombination mit den schlechten Radioteilen, die gerade bei 11g erheblich in Nachbarkanäle strahlen, kann auf dieser Basis kein Ersatz für ein Kabelgebundenes Netzwerk erreicht werden. Aus Sicht der Hersteller ist das optimal, führt das doch beim Kunden zum Paralleleinsatz von Wireless und traditionellen Produkten. Also zu einer Maximierung des Umsatzes.

Ich möchte an dieser Stelle noch einmal die Sichtweise von ComConsult-Research unterstreichen: Wireless Netzwerke sind eine Infrastruktur-Technologie, die auf einen Zeitraum von 5 Jahren den Einsatz kabelgebundener Netzwerke überflüssig machen wird. Die Kostenvorteile in der Installation aber auch im Betrieb (extrem niedrige Change-Kosten) werden bei mehr als 40% liegen (siehe unsere Studie zu diesem Thema).

Gleichzeitig ist Wireless eine Konvergenz-Technologie, da Anwendungsbereiche, die zurzeit getrennt realisiert sind, auf eine

Geleit

Technologie konzentriert werden. Dazu gehört vor allem Sprache (hier wird DECT von WLAN-Technik abgelöst werden), aber auch die Konstruktion kleiner Kommunikationsanlagen auf dieser Basis.

Trotz des Prognosezeitraums von 5 Jahren ist dies kein Traum in die Zukunft.

Unser Test von 11a/h-Produkten mit voller 200mW-Sendeleistung belegt eindeutig, dass ein Einstieg heute sinnvoll ist.

Es muss allerdings, wie der Schwerpunktartikel dieser Ausgabe zeigt, im Design und der Planung auf die zukünftig zu erwartende Entwicklung Rücksicht genommen werden. So können die heutigen Investitionen einerseits gesichert und andererseits gleichzeitig die Basis für eine wesentlich weiter gehende Wireless-Zukunft gelegt werden.

Unterstützt „ihr" Hersteller diese Entwicklung nicht, in dem er nur unzureichende 11a-Produkte anbietet, dann gibt es genügend Hersteller, die hier ein vollwertiges Produktangebot haben.

Wer an der Zukunft von Wireless-LANs Zweifel hat, der führe sich die Potenziale der 11i, 11e, 11f und 11n-Standards vor Augen. Hier ist eine Technologie entstanden, die deutlich mehr kann als einen Hotspot zu realisieren oder einen Konferenzraum zu versorgen.

Wir möchten dies im Detail und auch durchaus kontrovers mit Ihnen diskutieren. Das Wireless-LAN-Forum 2004 wird der Ort für diese spannende und voraussichtlich auch nicht immer einvernehmliche Diskussion sein. Ich würde mich freuen, wenn Sie dabei sind.

Ihr
Dr. Jürgen Suppan

Willkommen DATACOM-Magazin!

Wer in den 80er Jahren in den Datenkommunikations-Markt eingestiegen ist, der hat das Datacom-Magazin als die in Deutschland lange Zeit führende Fachzeitschrift für Datenkommunikation kennen und schätzen gelernt. Durch den mehrfachen Wechsel des Eigentümers und die damit verbundenen Änderungen der Ziele und Strategien der Inhaber verlor das Datacom-Magazin immer mehr an Bedeutung bis es im letzten Jahr eingestellt wurde. Viele der langjährigen Leser haben diese Entwicklung sehr bedauert, war doch speziell dieses Magazin über lange Jahre ein fester Bestandteil der eigenen beruflichen Entwicklung.

Nun ist das Datacom-Magazin zurück. Übernommen vom ehemaligen Redaktionsteam und unterstützt von vielen langjährigen Lesern erscheint es in Zukunft in veränderter Form als Web-Magazin. Das Magazin ist kostenfrei, erfordert aber eine Registrierung.

Das Team vom Netzwerk Insider wünscht dem Team des Datacom-Web-Magazin viel Erfolg auf dem Weg zurück zur alten Stärke.

Registrierungen zum Bezug des Web-Magazins können vorgenommen werden unter: www.datacom-magazin.de.

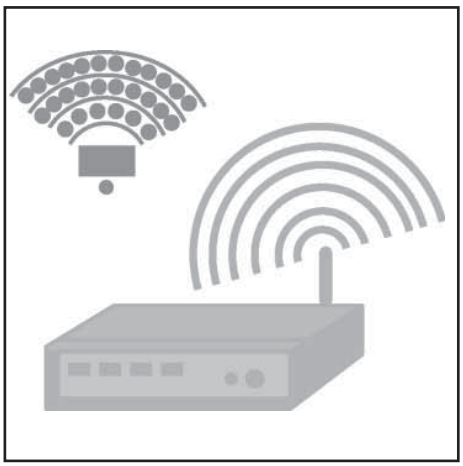
Top-Event

Wireless LAN Forum 2004

Das Wireless-LAN-Forum 2004 analysiert den Einsatz von Wireless-Netzwerken in der Praxis, stellt Planungs-Methoden gegenüber, vergleicht die heutigen und zukünftigen Wireless-Varianten, bewertet die Produkt- und Marktsituation und gibt Empfehlungen zum Betrieb und zum Trouble Shooting.

Im Einzelnen analysiert und diskutiert das WLAN-Forum 2004 folgende Themen:

- Die Zukunftssicherheit einer WLAN-Installation
- Umsetzung des neuen Sicherheitsstandards IEEE 802.11i
- Ist IEEE 802.11a einsatzbereit?
- Interoperabilität zwischen den Wireless-Standards



- Redundanz
- Planungsmethode
- Art der Teilnehmer
- Roaming
- Professioneller Betrieb
- Neubausituation
- Spezielle Anwendungsbereiche
- Hot-Spot-Anwendungen

Die Themenauswahl belegt: ein herausragender Kongress mit Top-Informationen, Analysen, Messergebnissen und Empfehlungen für die Planung und den erfolgreichen Betrieb von Wireless Netzwerken. Ein Kongress, den Sie nicht versäumen sollten. Sichern Sie sich rechtzeitig einen Platz für diese herausragende Veranstaltung.

Die letzten Tage!
Frühbucher-Rabatt bis 15.09.2004
Wireless LAN Forum 2004

Teilnahmegebühr vom 22.11. - 24.11.04 inklusive Report des Monats „Wireless LAN Evaluierung“ innerhalb der Frühbucherphase € 1.728,-- zzgl. MwSt. (regulär € 1.988,--zzgl. MwSt.)

Teilnahmegebühr vom 22.11. - 24.11.04 ohne Report „Wireless LAN Evaluierung“ innerhalb der Frühbucherphase € 1.430,-- zzgl. MwSt. (regulär € 1.690,--zzgl. MwSt.)

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden. Die Teilnahmegebühren werden mit Auslauf der Frühbucherphase fällig.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Wireless LAN Forum 2004

Ich buche den Kongress
Wireless Forum 2004
vom 22.11. - 24.11.04 in Königswinter

☐ **mit Report € 1.728,-- zzgl. MwSt.***

☐ **ohne Report € 1.430,-- zzgl. MwSt.***

***gültig bis 15.09.2004**

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Wireless LAN Forum 2004 - Programmübersicht

Montag, den 22.11.2004

9:30 - 11:00 Uhr

WLAN-Technologie in der Analyse: wohin wird die weitere Entwicklung gehen

- Datenraten, Reichweite
- Sicherheit, Anwendungen
- Voice over WLAN, Konkurrenz zum Kabel

Dr. F.-J. Kauffels, Unternehmensberater

11:30 - 12:30 Uhr

Markt- und Produktsituation

- Welche Märkte gibt es?
- Worin unterscheiden sich die Produkte?
- Was leisten die Hersteller, wie sind sie positioniert?
- Sind Konsumer-Produkte eine Alternative
- Ausblick auf die weitere Entwicklung

N.N.

14:00 - 15:30 Uhr

Security-Lösungen auf Basis von IEEE 802.11i und Vergleich mit den Alternativen

- Sicherheits-Risiken im WLAN
- Was leisten WPA und IEEE 802.11i: der neue Standard und die Folgen
- Pro und Kontra Security-Infrastruktur
- Zonenmodelle: pro und kontra
- WLAN als Security-Zone
- Alternativen: für wen ist was wann am besten geeignet (WPA/11i, IEEE 802.11x, VPN)
- Hot-Spot-Problematik und die Lösung
- Projekterfahrungen und Ausblick

Dipl.-Ing. Hans-Peter Mohn, ComConsult Beratung und Planung GmbH

16:00 - 17:00 Uhr

Redundanz-Konzepte in WLANs

- Wie entsteht Redundanz im WLAN
- Kernfrage: Zellüberlappung
- Resultierende Kapazitätsplanung
- Redundanzproblematik bei 11b und 11g
- Potenziale von 11a/h
- Spezielle Architekturen ausgewählter Hersteller
- Wie kann eine integrierte Konzeption mit dem Kabel-LAN erreicht werden

Dr.-Ing. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 23.11.2004

09:00 - 10:00 Uhr

Professioneller Betrieb und Management von WLANs

- Einmessung von Funkzellen
- Abnahme einer WLAN-Installation
- Spezialtools für die Planung
- Betriebs-Aufgaben und ihre Umsetzung
- Was tun bei Ausfällen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:00 - 10:45 Uhr

Vom Site-Survey zum Trouble-Shooting: Air Magnet

- Anforderungen an die Planung
- Was muss ein Planungstool leisten
- Site-Survey von AirMagnet
- Analyse und Trouble Shooting einer WLAN-Installation
- Anforderungsspektrum
- Die Air-Magnet-Familie

Eberhard Kaum, Netcor GmbH

11:15 - 12:00 Uhr

Betriebsoptimierte WLAN-Produkte

N.N.

12:00 - 14:45 Uhr

Planung einer WLAN-Installation

- 11a das unbekannte Wesen: Umgang mit DFS und TPC
- 11a oder 11g: Entscheidungskriterien
- Integrations ins Kabel-LAN
- Service-/Frequenzplanung
- Umgang mit Spezialfunktionen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr

Erstellung einer WLAN-Ausschreibung

- Aufbau der Ausschreibung
- Vorgabe von Qualitäten, Vorgehensweise
- Projekt-Erfahrungen, Besonderheiten

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:00 - 16:45 Uhr

Voice over WLAN

- Bedarf und typische Anwendungsbeispiele: Telefonieren im WLAN
- Einbindung in eine IP-Telefonie-Lösung
- Testerfahrung mit WLAN-Telefonen
- Andere Planung gefordert: Zellüberlappung und Roaming
- Kernthema: Quality of Service
- Handhabung der Sicherheits-Anforderungen
- Szenario 1: 11b/g, Szenario 2: 11a
- Ausblick: wird DECT durch diese Technik verdrängt?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

16:45 - 17:30 Uhr

Neubausituation: WLAN kontra Kabel oder die Suche nach der optimalen Mischung

- Vergleichbarkeit der Planungsansätze
- Alternative 1: Reiner Kabelansatz
- Alternative 2: Reiner WLAN-Ansatz
- Alternative 3: Overlay-Network
- Vergleich der Alternativen
- Kosten und Betriebstrends
- Empfehlung für die Neubausituation

N.N.

10:45 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Mittwoch, den 24.11.2004

9:00 - 10:00 Uhr

Von der Architektur zum Betrieb: professionelle Umsetzung von WLAN-Lösungen

- Architektur-Varianten
- Typische Probleme und Randbedingungen
- Elemente eines professionellen Betriebs
- Neue Technologien und ihre Nutzung

Cisco Deutschland GmbH

10:00 - 11:00 Uhr

Wireless LAN im Produktions-Umfeld

- Potenziale der WLAN-Technik im Produktionsbereich
- Anwendungsbeispiele
- Rahmenbedingungen des Umfelds
- Anforderungen an ein WLAN
- Lösungsportfolio von Siemens

Siemens AG

11:30 - 12:30 Uhr

Kompatibilität-Architektur zwischen den WLAN-Standards

- Ausgangslage: gegenseitige Beeinflussung von 11b, 11g, 11a
- Handhabung von 11b-Clients in einer 54 Mbit/s-Umgebung
- Kompatibilitäts-Methoden und ihre Nutzung
- Vermeidung der Benachteiligung von 11g
- Aufbau einer Kompatibilitäts-Architektur
- Betriebsaspekte, Empfehlungen

Dr. F.-J. Kauffels, Unternehmensberater

14:00 - 14:45 Uhr

Roaming

- Roaming: Bedarf und Anforderungen
- Auswirkungen auf die Planung: Handhabung von Zellüberlappungen
- Was leistet der Standard IEEE 802.11f, wie sind Produkte auf der Basis diese Standards zu bewerten
- Messergebnisse
- Konsequenzen
- Herstellerspezifische Lösungen

Dr.-Ing. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:45 - 15:45 Uhr

Planung und Betrieb eines Hot-Spots

- Funktechnische Auslegung
- Einwahl, Abrechnung
- Verkehrssteuerung
- Sicherheit, Überwachung und Betrieb

Dr.-Ing. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause

Der Veranstalter behält sich Änderungen im Programm vor!

Kommentar

Windows XP Service Pack 2: das Problem heißt nicht Microsoft

von Dr. Jürgen Suppan

Die Meldungen um Unverträglichkeiten mit XP Service Pack 2 (SP2) reißen nicht ab. Die Liste der betroffenen Programme wird immer länger. Im Mittelpunkt der Diskussion steht die Firewall, die naturgemäß die Kommunikation nicht definierter Anwendungen blockiert (man beachte: dies ist die Aufgabe einer Firewall). Und weil es so schön üblich und auch einfach ist, überschlagen sich weltweit Journalisten und viele Anwender mit der Microsoft-Schelte. Dabei ist diese Schelte und der Umfang der Kritik in keiner Weise mehr akzeptabel.

Auch wenn mir nicht alles an SP2 gefällt (ich hätte mir vor allem eine stärkere Modularität gewünscht), so möchte ich aus Sicht von ComConsult-Research klar stellen: Microsoft hat mit SP2 einen wichtigen und richtigen Schritt getan, der längst überfällig war. Auch dieser Schritt wird nicht alle Sicherheitsprobleme und alle potenziellen Lücken beseitigen, aber er reduziert die Angriffsfläche doch erheblich.
Nun wird Service Pack 2 von einer Reihe von Anwendern offenbar wie ein normales Update behandelt und ungeprüft eingespielt. Dazu ist anzumerken, dass SP2 jetzt zwar als „normales“ Update zur Verfügung steht, aber grundsätzlich wie ein neues Major-Release zu behandeln ist. Wer sich nach der Installation von SP2 auf dem PC eines Endanwenders beschwert, dass diverse Anwendungen nicht laufen, der sollte sich selbstkritisch die Frage nach der eigenen Professionalität stellen.

Professioneller PC-Betrieb sollte unverzichtbar ein zentrales Testcenter beinhalten, das die gängigen im Unternehmen vorhandenen Installations-Profile beinhaltet und den Test der Nutzbarkeit aller vorhandenen Anwendungen ermöglicht. Parallel sollte gerade bei der Kombination aus Windows XP beim Client und aus Windows 2003 Server ein zentralisierter und automatisierter Betrieb unterstellt werden. Der Sinn dieser Client-Server-Konstellation liegt ja gerade in der Nutzung der erweiterten Gruppenrichtlinien und der damit verbundenen Umsetzung eines zentralen Konfigurations-Managements. Wer diese Konstellation ohne diese Möglichkeiten betreibt, der hat im Wesentlichen sinnlos Geld vernichtet. Natürlich kann es nicht das Ziel sein, dass jeder Anwender jetzt anfängt, an seiner Firewall-Definition Änderungen vorzunehmen. Das mag für Konsumer durchaus notwendig und unvermeidbar sein, doch für diese gibt es entsprechende Produkte, die sehr angenehm zu konfigurieren sind. Im Unternehmen gilt: kein Endanwender ändert irgend etwas an der Konfiguration seines PCs. Schon gar nicht installiert er neue Programme (auch wenn der Anwender im Vorstand sitzt).

Ich bleibe bei meinem Standpunkt:

- Natürlich sind mit SP2 ggf. Probleme verbunden. Diese werden vor allem in unlösbarer Form Applikationen betreffen, die mit den Einschränkungen des neuen Speicher-Managements nicht klar kommen. Auch hier liegt die Ursache nicht bei Microsoft sondern bei Herstellern, die schlecht programmierte Anwendungen herausgeben
- Natürlich ist es peinlich, dass auch Microsoft-eigene Anwendungen nicht laufen. Auch hier gilt, dass wohl bei der Programmierung der Anwendungen vom rechten Weg abgewichen wurde
- Ansonsten kann niemand, der über einen Testbetrieb verfügt, der die Konfiguration seiner Client-PCs zentral steuert und genau im Griff hat und die Gruppenrichtlinien in der gesamten Breite ihrer Möglichkeiten nutzt (trotz der wenig nachvollziehbaren Bediensystematik) wirklich mit SP2 in ein Problem laufen
- Es ist auch nicht auszuschließen und auch zu erwarten, dass in SP2 noch Probleme auftauchen, ggf. hat Microsoft auch das Release durch den hohen internationalen Druck und die Kritik an der häufigen Verschiebung zu früh heraus gegeben. Da aber vor dem Einsatz von SP2 umfangreiche Tests im Testcenter erforderlich sind, werden vor der unternehmensinternen Freigabe sowieso mehrere Wochen vergehen. Bis dahin wird der Status seitens Microsoft klar sein
- SP2 sollte in der Einführung auf jeden Fall wie ein Major-Release behandelt werden. Eigentlich ist es eine neue Betriebssystem-Version. Zu umfangreich sind die Änderungen auch bei Kernkomponenten des Betriebssystems. Auf keinen Fall darf es wie ein einfaches Update behandelt werden

Auch ich ärgere mich gelegentlich über Microsoft, vor allem im Bereich der Lizenzpolitik, die klar den Eindruck des Ausnutzens einer Monopolposition hinterlässt. Aber mir hängt es langsam wirklich zum Halse raus, dass viele Leute, die jede Form eines professionellen Betriebs vermissen lassen, permanent nur die Schuld bei Microsoft suchen. Windows XP Service Pack 2 ist eines der besten und modernsten Betriebssysteme, die es je für ein Endgerät gegeben hat. Es ist komplex und beinhaltet deshalb Tücken und auch Fehler (wie alle guten und begrüßenswerten Alternativen auch). Das war noch bei keinem Betriebssystem in der Vergangenheit anders und wird auch in Zukunft nicht anders sein. Diese Komplexität ist der Preis für eine zentrale Betreibbarkeit, für einen hohen Grad an Sicherheit und für eine breite Nutzbarkeit für verschiedenste Typen und Architekturen von Anwendungen.

Gerade die Diskussion um Windows XP Service-Pack 2 zeigt wieder einmal, dass die Grundelemente eines professionellen Betriebs auch und gerade für PCs unverzichtbar sind:

- Trennung von Operativ- und Testbetrieb, wobei für den Testbetrieb alle existierenden Konfigurationen nachgebildet werden können müssen. Schon dies schließt individuelle Installationen komplett aus
- Aufbau eines zentralen Konfigurations-Managements
- Aufbau eines zentralen Update-Managements als Teil des Konfigurations-Managements
- Der Personalschwerpunkt darf nicht im Vor-Ort-Konfigurations-Management liegen, er muss eindeutig im Bereich eines zentralisierten und automatisierten Betriebs angesiedelt sein. So müssen insbesondere für den Testbetrieb ausreichende Personalressourcen und auch Sachmittel zur Verfügung stehen. Dies ist immer hochgradig wirtschaftlich und Kern jeder wirtschaftlichen Optimierung

Wer diese einfachen und nicht neuen Grundregeln, die ja gerade mit der Einführung von Windows 2000 endlich auch im PC-Betrieb durch eine Zentralisierung des Konfigurations-Managements umsetzbar wurden, einhält, der hat auch mit SP2 keine Überraschungen zu erwarten. Der Hauptaufwand konzentriert sich auf den Testaufwand. Der ist nicht niedrig, entspricht aber dem Charakter von SP2 als „Major-Release“.

In diesem Sinne viel Spaß beim Testen
Dr. Jürgen Suppan

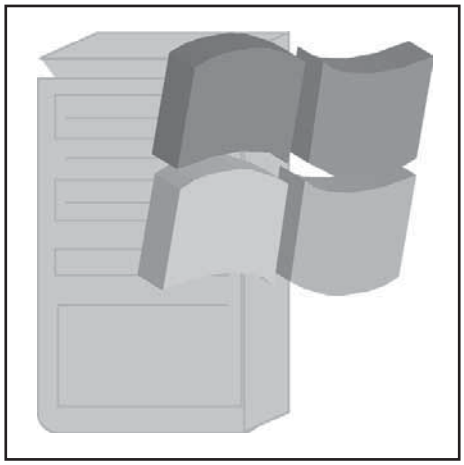
Aktuelle Sonderveranstaltung

NEUES SEMINAR: Migration von Windows NT nach Server 2003 - Strategische Entscheidungen

Vom 04. - 05. Oktober 2004 veranstaltet die ComConsult Akademie in Köln zum ersten Mal das 2-tägige Seminar „Migration von Windows NT nach Server 2003 - Strategische Entscheidungen“.

Dieses Seminar zeigt insbesondere Entscheidern Neuerungen aus Windows Server 2003 im Bereich des Verzeichnisdienstes Active Directory (Version 2) und des IP-Managements, welches für neue Landschaften im Windows-Umfeld die infrastrukturellen Rahmenparameter liefert. Ferner werden strategische Entscheidungen, die mit der Migration von Windows NT nach Windows Server 2003 verbunden sind, erläutert und so vorbereitet, dass die Entscheider in die Lage versetzt werden, die für ihr Unternehmen richtige Entscheidung zu treffen.

Ende dieses Jahres endet die Extended Support Phase von Microsoft für Windows NT Server. Für Unternehmen, die noch Windows NT Server produktiv im Einsatz haben, ist dies ein kritisches Datum, da dann auch das kostenlose Update mit Sicherheitspatches wegfällt.



In einem Teil des Seminars wird auch die Clientlandschaft (insbesondere mit Windows XP) in die Überlegungen einbezogen. Hierbei liegt das Hauptaugenmerk auf der Schaffung von Standards zur Generierung einer effizient zu administrierenden homogenisierten Landschaft.

Sie lernen in diesem Seminar

- wie eine Migration nach Windows Server 2003 vorbereitet wird
- welche technischen Aspekte dabei zu beachten sind
- welche Wahlmöglichkeiten auf der 2003 Server Seite bestehen, welche Vor- und Nachteile mit den einzelnen Aspekten verbunden sind
- was beim Aufbau einer geeigneten und zukunftsorientierten Active Directory Struktur zu beachen ist
- welche unbedingt zu beachtenden technischen Abhängigkeiten zu anderen technischen Systemen, insbesondere DNS und IP-Management bestehen
- wie Sie diese Abhängigkeiten im Sinne eines geschlossenen und tragfähigen Gesamtkonzepts verarbeiten
- welche typischen Fallen bei der Migration existieren und wie Sie diese umgehen
- wie die Migration von der Planung bis zur Umsetzung wirtschaftlich optimal abgewickelt wird

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Migration von Windows NT nach Server 2003 - Strategische Entscheidungen

Ich buche das folgende Seminar in Köln:

☐ **Migration von Windows NT nach Server 2003 - Strategische Entscheidungen**
04.10. - 05.10.04
(Preis € 1.390,-- zzgl. MwSt.)

☐ Buchen Sie für mich ein Hotelzimmer

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

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

Zweitthema

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

Dr.-Ing. Joachim Wetzlar ist seit mehr als 10 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH. Er leitet dort das Competence Center „Trouble-Shooting und Messtechnik“ und ist maßgeblich an seinem Aufbau beteiligt. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netz-Redesigns und WLAN-Planungen durch.

Fortsetzung von Seite 1

Zum anderen verbirgt sich hinter Protokollanalyse immer auch ein Messgerät, das im Allgemeinen groß, schwer und furchtbar teuer ist. Vielleicht verstaubt ja auch bei Ihnen ein DA30, Internet Advisor oder K1100, weil seine Bedienung viel zu kompliziert ist und niemand Zeit hat (bzw. von seinem Chef zugeteilt bekommt), seine Bedienung zu erlernen. Wie schön wäre es, wenn man einen einfachen und zugleich leistungsfähigen Protokollanalysator ständig zur Hand hätte, mit dem man einfach mal zwischendurch eine Messung machen kann, so wie man eine Mail schreibt. Am besten wäre hierfür natürlich ein kostenloses Produkt.

Bei der Suche stößt man unweigerlich auf Ethereal, das bekannteste und beste Open-Source-Produkt zur Protokollanalyse. Ethereal wurde 1997 von Gerald Combs entwickelt, der 1998 die erste Version 0.2.0 veröffentlichte. Seither ist eine ständig wachsende Gemeinde im Internet an der Weiterentwicklung von Ethereal beteiligt. Besonders der Entwurf neuer Protokolldekoder („Dissectors“) hat seither viele Menschen beschäftigt, und hier wird der Nutzen der Open-Source-Gedanken besonders deutlich: Wer ein spezielles Protokoll messen und darstellen möchte, schreibt sich einen entsprechenden Dekoder. Und veröffentlicht ihn dann für die Allgemeinheit! Jedes Protokoll zwischen Layer 2 und 7, das von seinen Entwicklern offen gelegt wurde, lässt sich wahrscheinlich auch mit Hilfe von Ethereal dekodieren. Wer also sicher stellen möchte, dass in seinem Unternehmensnetz ausschließlich offen gelegte Protokolle einsetzt werden, fordert von seinen Lieferanten die Unterstützung aller von den angebotenen Systemen verwendeten Protokolle durch Ethereal.

Ethereal befindet sich aus der Sicht eines Software-Entwicklers immer noch im „Beta-Stadium“. Der Anwender muss also auch schon mal mit Fehlern rechnen. Seit Dezember 2003 (Version 0.10.0) hat die Benutzeroberfläche jedoch so große Fortschritte gemacht, dass Ethereal alle „althergebrachten“ Protokollanalysatoren für Windows PC (Sniffer, EtherPeek, Observer, Surveyor, etc.) ersetzen kann. Wir jedenfalls nutzen die Software inzwischen immer öfter zur Fehlersuche bei unseren Kunden und führen auch die Zertifizierung zum ComConsult Certified Trouble Shooter auf Basis von Ethereal durch.

1. Installation

Ethereal bekommt man auf der Web-Seite http://www.ethereal.com. Die Homepage nennt die gerade aktuelle Version - Anfang Juni 2004 ist es die Version 0.10.4. Unter dem Link „Download“ findet man die Quelldateien und übersetzte Versionen für die verschiedensten Betriebssysteme. Die Vorgehensweise zur Installation unter Li-

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

nux beschreibe ich am Ende, wenn es um die WLAN-Analyse geht. Auch die Version für Solaris habe ich schon erfolgreich installieren können (geht problemlos mittels „pkgadd"). Hier beschränke ich mich zunächst auf die Windows-Version. Benötigt wird die Datei „ethereal-setup-0.10.4.exe", die nach erfolgreichem Download (ca. 8 MByte) ausgeführt wird. Es erscheint der „Ethereal Setup Wizard" ganz im Stil des modernen Windows. Die Taste „Next" führt zum unvermeidlichen License Agreement; hier handelt es sich um die GNU General Public License. Lesen Sie mal die Präambel: „Während die meisten Lizenzen gemacht wurden, um Ihre Rechte zur Verteilung und Veränderung einzuschränken, wird Ihnen dieses Recht hier garantiert..". Man wird also „I Agree" drücken und gelangt zur Komponentenauswahl. Hier kann man im Pull-Down-Menue „Select Type of Install" zwischen „GTK2" und „legacy GTK1" wählen. Was hat es damit auf sich? GTK ist eine Software-Bibliothek, die Bausteine für graphische Benutzeroberflächen enthält. Menüs, Knöpfe und Rollbalken stammen bei Ethereal also nicht von Microsoft, sondern aus GTK. GTK2 ist die modernere Variante mit mehr Möglichkeiten (z.B. hübschere Knöpfe), hat aber unter Windows noch einige Fehler, z.B. bei der Fensterverwaltung. Ich empfehle also derzeit noch „legacy GTK1". Man drückt „Next" und nach kurzer Zeit ist Ethereal installiert.

Aber halt! Da fehlt noch ´was. Ethereal kann in dieser Form lediglich dazu verwendet werden, zuvor mit irgend einem anderen Analysator aufgezeichnete Dateien (Trace-Files) anzuzeigen. Um mit Ethereal tatsächlich messen zu können, ist ein spezieller Treiber zu installieren, der unter der Bezeichnung „WinPcap" bei http://winpcap.polito.it zu finden ist. Die aktuelle Version heißt „WinPcap_3_1_beta_3.exe". Sie simuliert die in UNIX-Betriebssystemen zur Paketaufzeichnung allgemein verwendete „libpcap" unter Windows. Auch hier heißt es, die EXE-Datei einmal auszuführen und sich durch den „Wizard" leiten zu lassen; spezielle Optionen sind nicht einzustellen. Eventuell muss abschließend der Rechner einmal neu gestartet werden.

Als abschließenden Installationsschritt empfehle ich, Ethereal einmal zu starten („Programme > Ethereal > Ethereal") und *Edit > Preferences* auszuführen. In der linken Dialogbox wählt man *Font* und stellt eine Schriftart ein. Ich finde *Lucida Console, size 10* am übersichtlichsten. Außerdem empfehle ich, eine Spalte mit der Paketgröße hinzuzufügen, da man diese Information bei der Protokollanalyse immer wieder braucht. Man wählt *Columns* und dann *New*. In der Zeile Title gibt man eine Bezeichnung ein, z.B. *Size*, drückt auf *Format* und sucht nach *Packet length (bytes)*. Mit Up schieben Sie die Spalte an die gewünschte Stelle, ich empfehle zwischen *Time* und *Source*. Abschließend drückt man *Save* und *Ok*. Dadurch wird ein Verzeichnis mit Konfigurationsfiles angelegt, die für die spätere Arbeit recht nützlich sind. Beispielsweise merkt sich Ethereal darin die zuletzt geöffneten Dateien. Jetzt haben Sie schon ein wenig Erfahrung im Umgang mit den Menüs von Ethereal bekommen. Wichtig ist es, den Unterschied zwischen *Ok* und *Save* immer im Kopf zu behalten: *Ok* wendet die Einstellungen an, speichert sie aber nicht ab. Beim nächsten Start von Ethereal sind die Einstellungen also verloren – es sei denn, Sie hatten sie zuvor mittel *Save* gesichert. Die neue Spalte sieht man übrigens erst, nachdem Ethereal einmal neu gestartet wurde.

2. Paketaufzeichnung

Nun hat man einen vollwertigen Protokollanalysator auf seinem Rechner installiert. Versuchen Sie einfach mal, etwas aufzuzeichnen. Drücken Sie dazu in Ethereal den ganz linken Knopf in der Werkzeugleiste, der mit dem Zahnrad - oder die Tatenkombination Ctrl+k. Es erscheint ein Dialogfeld mit „Capture Options". Nichts verändern, sondern nur in der obersten Zeile das Interface einstellen, an dem das LAN angeschlossen ist und *Ok* drücken. Jetzt werden alle Daten aufgezeichnet und man sieht eine kleine Statistik der gefundenen Protokolle. Mit *Stop* hält man die Aufzeichnung an und die Pakete sind zu sehen. Neben der Ihnen bekannten Netzwerkkarte fällt auf, dass man einen „Generic NdisWan adapter" einstellen kann. Er dient zur Messung auf WAN-Schnittstellen, wenn Sie z.B. eine Internet-Verbindung über eine ISDN-Karte hergestellt haben und sehen wollen, was sich da so alles tut.

Noch einmal zurück zu den „Capture Options". Neben der Netzwerkkarte lassen sich hier noch zahlreiche weitere Optionen auswählen. Für erwähnenswert halte ich die folgenden Punkte:

- *Enable Network Name Resolution*: Markiert, versucht Ethereal, alle IP-Adressen über den DNS-Server in Namen umzuwandeln. Und das kann dauern! Lassen Sie diese Option bitte deaktiviert.

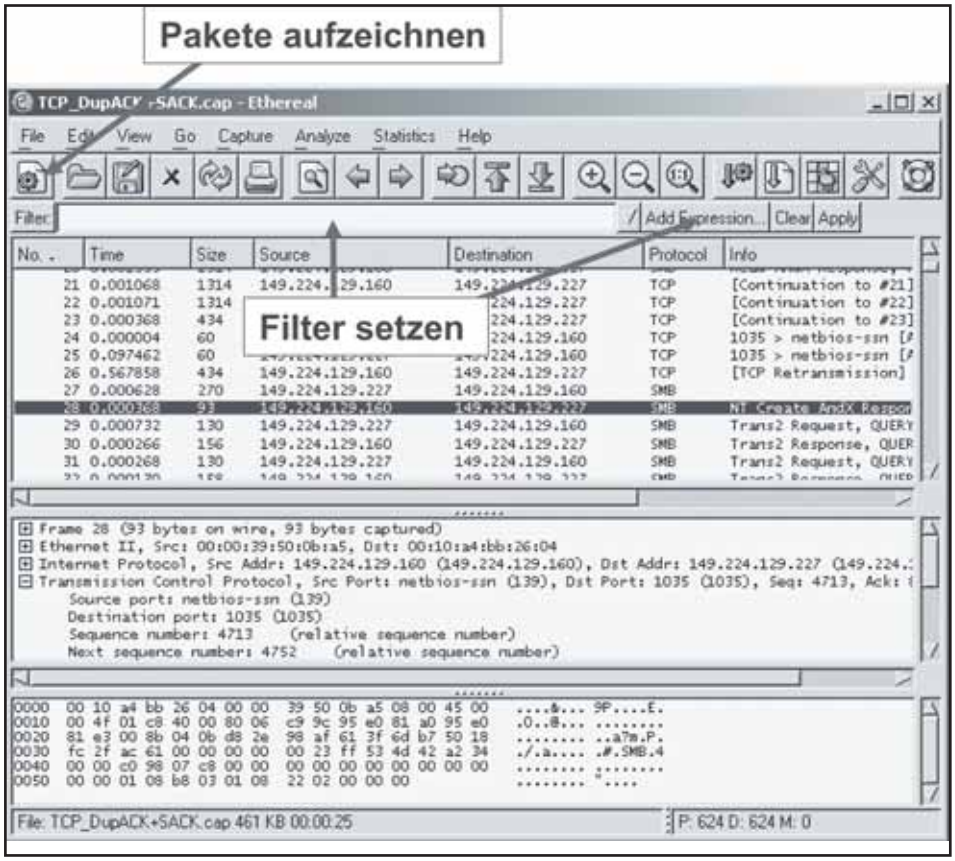


Abbildung 1

- *Update list of packets in real time* in Kombination mit *Automatic scrolling*: Ethereal zeigt alle Pakete an, sobald sie aufgezeichnet wurden. Das funktioniert natürlich nur, wenn die Netzlast gering ist.

- *Limit each packet to xx bytes* erlaubt es, nur die Paket-Header aufzuzeichnen und den meist langen Datenteil zu verwerfen. Dadurch lässt sich kostbarer Speicherplatz bei der Aufzeichnung sparen. Ein sinnvoller Wert für „xx“ ist 256 Byte. Kleinere Werte knabbern zuweilen auch lange Header an, z.B. bei bestimmten SMB-Paketen.

- *Capture Filter* ist die wichtigste Option. Sie erlaubt es, Pakete schon vor der Aufzeichnung zu qualifizieren. Unerwünschte Pakete gelangen dann gar nicht erst in den Speicher. Wie man mit den Filtern umgeht, beschreibe ich weiter unten.

Sind die Pakete erst einmal aufgezeichnet, kann man sie mit Ethereal auf verschiedene Weisen betrachten, noch einmal filtern sowie verschiedenen statistischen Analysen unterziehen. Selbstverständlich kann man sie auch für spätere Analysen in Dateien abspeichern. Unter *File > Save* erscheint das entsprechende Menü, in dem man Pfad und Dateiname einstellt. Achtung, das Look-and-Feel ist alles andere als Windows und man muss sich erst daran gewöhnen. Schauen Sie mal unter *File type*: nach. Hier lässt sich eine Vielzahl von Dateiformaten einstellen und Ethereal ist in der Tat kompatibel zu fast allen am Markt gängigen Protokollanalysatoren. Bisher habe ich Traces immer als „Sniffer 2.0“ abgespeichert, das verstehen die meisten Analysatoren. Selbstverständlich lassen sich auch Teile der Aufzeichnung oder einzelne Pakete abspeichern - die entsprechenden Optionen sind selbsterklärend.

3. Analyse der Paketinhalte

Der Protokolldekoder stellt Pakete in der allgemein üblichen Form in drei Bereichen dar. Oben findet man die Übersicht - eine Zeile pro Paket -, in der Mitte wird ein Paket im Detail dekodiert und unten sieht man die Hex-ASCII-Darstellung des Paketes. Die Bereich lassen sich mit der Maus anpassen und über *Edit > Preferences > Layout* anders anordnen oder ganz ausblenden. Eine schnelle Möglichkeit, einen Bereich auf den ganzen Bildschirm auszudehnen, fehlt leider. Hier könnte man sich z.B. am Sniffer orientieren, der dafür die Taste „F4“ kennt (wer programmiert ´s?).
Die Paketübersicht zeigt Paketnummer, Zeit, Quell- und Zieladresse, Protokoll und Zusammenfassung an. Und wenn Sie meiner Empfehlung von oben gefolgt sind, auch noch die Paketgröße. Suchen Sie mal das kürzeste Paket, indem Sie oben auf die Spaltenbezeichnung „Size“ klicken. Und dann das längste - noch mal klicken. Das funktioniert natürlich mit allen Spalten.

Die Spalte „Time“ erlaubt allerlei Zeitmessungen, wenn Sie z.B. mal wieder nachweisen müssen, dass der Server das langsamste Glied in der Kette ist und nicht das Netz. Über *View > Time display format* lässt sich z.B. *Seconds since previous packet* einstellen, die Zeit seit Ende des vorangegangen Pakets. Zur Demonstration führen Sie mal von Ihrem Rechner einen Ping auf ein entferntes System aus und zeichnen sie das ganze mit Ethereal auf. Markieren Sie ein „Echo reply“, das unmittelbar auf ein „Echo request“ folgt. Die Zeitangabe nennt die Round-Trip-Time, also die Laufzeit des Ping zum Ziel und die Antwort vom Ziel zu Ihnen zurück. In Kombination mit der Paketlänge kann man nun beispielsweise den Durchsatz ausrechnen, unter der Voraussetzung, dass das Ziel ohne Zeitverzug geantwortet hat. Was aber, wenn die beiden Pakete, deren zeitlichen Abstand man messen möchte, nicht unmittelbar hintereinander stehen. Dann stellt man die Zeitmessung auf *Seconds since beginning of capture.* Man markiert das erste Paket mit der rechten Maustaste und wählt *Time reference > Set time reference (toggle)*. Nun werden die Zeiten der nachfolgenden Pakete bezogen auf diese Referenz ausgerechnet.

4. Filtern, aber richtig

Wie bereits erwähnt, lassen sich Datenpakete bei der Aufzeichnung bereits filtern (Capture Filter). Aber auch nachträglich lassen sich Pakete aus der Aufzeichnung herausfiltern. Wenn Sie nicht genau wissen, worin das Netzproblem eigentlich besteht, zeichnen Sie erst mal über einen gewissen Zeitraum alle Daten auf und filtern nachträglich zum Beispiel alle http-Anfragen, alle Pakete einer bestimmten

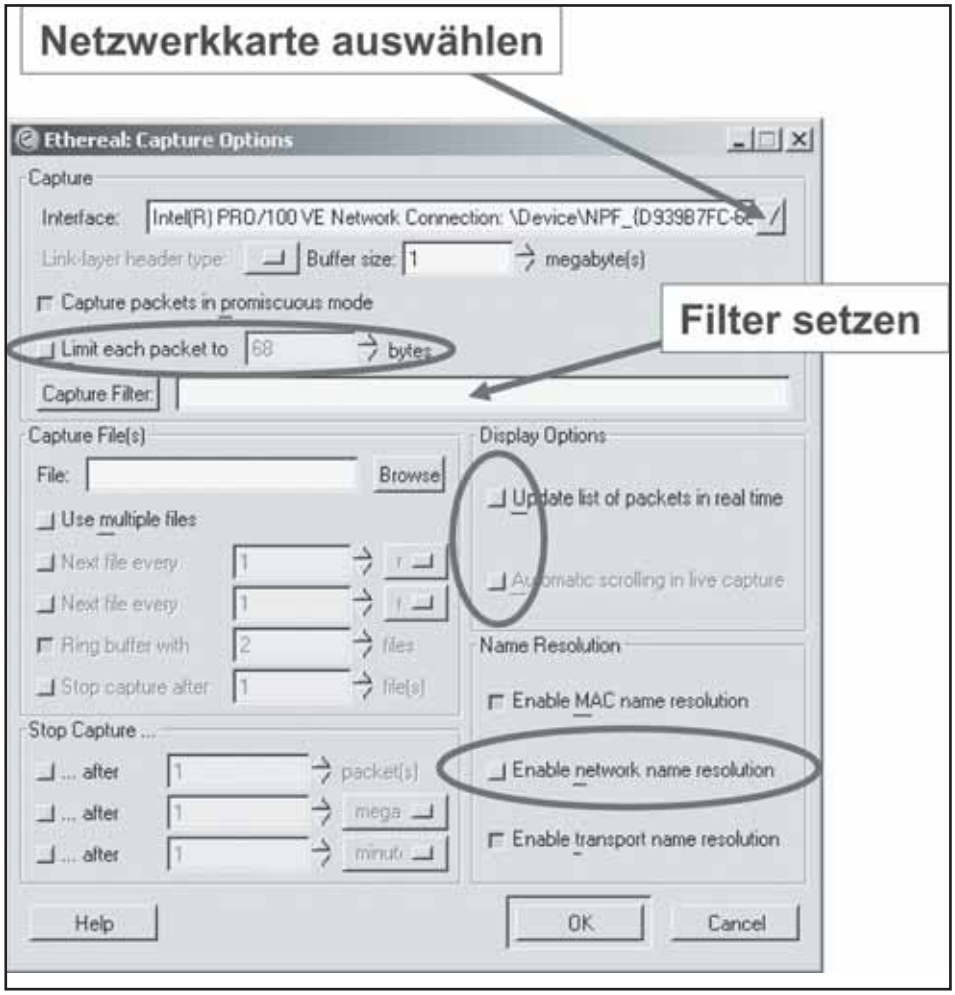


Abbildung 2

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

IP-Station, alle Pakete einer bestimmten TCP-Sitzung, usw. heraus. Hier zeigt Ethereal seine eigentliche Stärke. Die Möglichkeiten, Display-Filter zu setzen, sind einzigartig - vielleicht noch erreicht durch das „Examine“ von Acterna. Auf Grund der Trennung von Paketaufzeichnung und -Anzeige haben sich zwei unterschiedliche Konzepte der Filtereinstellung ergeben, die ich kurz beschreiben möchte:

- Capture-Filter verwenden die Syntax der UNIX „libpcap“, wie sie z.B. in der Manual-Page von „tcpdump“ beschrieben wird. Die am häufigsten verwendeten Filter werden sein *ether host 08:AF:08:15:47:11* für MAC-Adressfilter oder *host 192.168.0.10* für IP-Filter. Die Ethereal-Hilfe gibt eine für die Praxis ausreichende Beschreibung.

- Display-Filter erlauben die Angabe beliebiger Felder in beliebigen Protokollen, also z.B. „*ip.ttl*“ oder *tcp.port*. Diese Felder werden mit Werten verglichen (gleich, ungleich, kleiner, etc.) und lassen sich logisch (und, oder, nicht) verknüpfen. Der Filter für eine TCP-Sitzung sieht dann z.B. folgendermaßen aus: (*ip.addr == 10.2.2.1 && ip.addr == 10.5.5.3*) && (*tcp.port == 21 && tcp.port == 1455*).

  Da man das nicht alles im Kopf behalten kann, gibt es einen „Wizard“, den man durch Drücken der Taste *Expression...* erreicht. Hier sind alle Protokolle mit ihren Feldern, die Relationen und möglichen Vergleichswerte aufgeführt. Versuchen Sie mal einen Filter auf das PUSH-Bit zu setzen: Suchen Sie unter TCP nach *Push,* wählen Sie als Relation == und dann *Set*. Das gleiche erreichen Sie im Übrigen auch direkt aus der Protokollanalyse. Klicken Sie mit der rechten Maustaste auf ein Feld in der Detaildarstellung eines Pakets (z.B. wieder auf das PUSH-Bit im TCP). Es öffnet sich ein Kontextmenü, in dem Sie unter *Apply as Filter* oder *Prepare a Filter* verschiedene Möglichkeiten haben. *Selected* schreibt einen Filter für das angeklickte Feld unmittelbar in die Filter-Zeile und wendet ihn auch gleich an, sofern Sie „Apply...“ gewählt hatten. Probieren Sie auch mal die anderen Optionen aus.

Sehr oft wird man auf bestimmte TCP-Sitzungen filtern müssen. Das geht am einfachsten, indem man mit der rechten Maustaste auf ein beliebiges Paket der Sitzung klickt und *Follow TCP stream* auswählt. Zusätzlich öffnet sich dann ein Fenster, das den gesamten Inhalt der Kommunikation in ASCII, EBCDIC oder

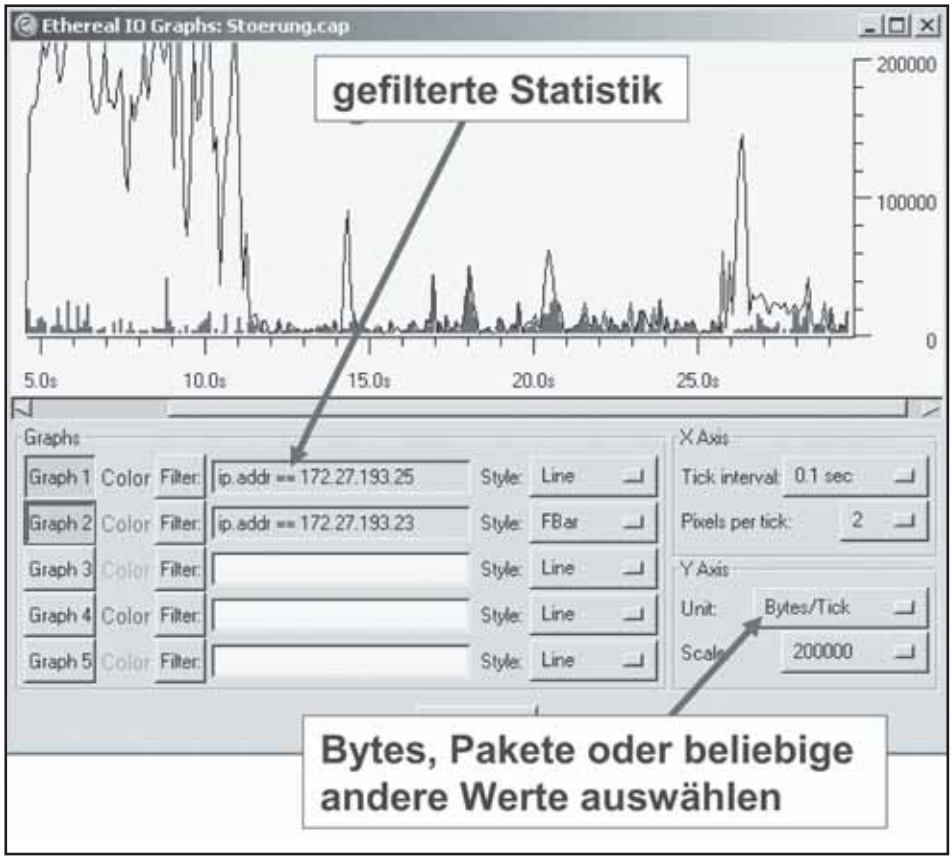


Abbildung 3

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

Hex-Dump zeigt. Damit lässt sich z.B. der Inhalt einer TN3270-Sitzung im Klartext anzeigen. Oder man kann eine im Netz übertragene Datei als ganzes zurückgewinnen und sogar abspeichern(!).

5. Statistiken

Für viele Messaufgaben braucht man eher statistische Analysen als genaue Kenntnis der Paketinhalte. So will man beispielsweise erfahren, wie sich die Auslastung einer WAN-Strecke im Tagesverlauf verändert hat, welches die Top-Talker sind oder welche mittlere und maximale Antwortzeit eines Servers in der vergangenen Stunde beobachtet wurde. Für Langzeitstatistiken gibt es andere Open-Source-Produkte, wie MRTG oder NTop. Ethereal kann nur seine Trace-Files statistisch analysieren. In der Praxis kann ein Trace-File kaum mehr als 100 MByte groß sein, das entspricht einem Zeitraum von ca. 1 Minute bei 100 MBit/s und 10% Netzlast. Dafür sind die Statistiken aber umfangreicher und haben einen direkten Bezug zum Trace. Beispielhaft seien hier drei nützliche Statistiken genannt, die sich im Menü *Statistics* finden lassen:

- *IO Graphs* stellt bis zu 5 Auslastungskurven in einem Diagramm dar. Das klingt zunächst ganz normal, aber die Möglichkeiten sind verglichen mit anderen Protokollanalysatoren einmalig. Man kann nämlich nicht nur vordefinierte Werte anzeigen, sondern für jeden Graphen beliebige Filter setzen. So lässt sich z.B. die Zahl der TCP-Retransmissions auf einer WAN-Strecke der Datenrate gegenüberstellen, um hier eine eventuelle Abhängigkeit nachzuweisen. Oder man vergleicht die Auslastung zweier Server miteinander und stellt fest, dass am einen die Datenrate einbricht und am anderen nicht (siehe Bild). Es lassen sich sogar beliebige Parameter als Funktion der Zeit darstellen: Man stellt unter *Y Axis > Unit die Option Advanced...* ein und erhält ein neues Feld pro Graph (und zunächst eine Fehlermeldung, weil man noch nichts eingegeben hat...). Wenn man in das Feld z.B. *frame.time_delta* eingibt und unter Calc: *LOAD(*)* auswählt, wird die Verteilung der Delta-Zeiten angezeigt. Wählt man dann noch einen geschickten Filter aus, z.B. für einen ICMP Echo-Reply (*icmp.type == 0*), lassen sich mit Hilfe eines Ping auf einfache Weise Round-Trip-Zeiten messen und graphisch darstellen.

- *Conversation List* zeigt alle Kommunikationspaare des ausgewählten Protokolls In der Praxis wird man wahrscheinlich häufig *Ethernet, IPv4* und *TCP* verwenden. Will man sich eine bestimmte Kommunikation näher ansehen, klicke man mit der rechten Maustaste auf den Eintrag und setze ein Filter; das Kontextmenü funktioniert genauso wie bei den Display-Filtern beschrieben.

- *Service Response Time* rechnet kleinste, mittlere und längste Antwortzeiten von Layer-7-Protokollen aus. Besonders interessant finde ich SMB mit seinen zahlreichen Kommandos. Damit konnten wir einst ein vermeintliches Netzproblem stattdessen in der SAN-Anbindung eines Servers identifizieren. Die Statistik zeigte bei den typischen Kommandos für Dateizugriffe (ReadAndX, Close, etc.) maximale Antwortzeiten von 15 Sekunden, während die für die Sitzungskontrolle verantwortlichen (SessionSetupAndX, Tree-ConnectAndX, etc.) immer unter 100 Millisekunden lagen.

6. Hat Ethereal einen Expertenmodus?

„Um Gottes Willen - nein!“, wird man Ihnen bei den etablierten Herstellern erzählen. Lassen die sich doch ihre so genannten Experten im Allgemeinen teuer bezahlen. Aber mal Hand auf´s Herz: Welche Funktionen des Experten benötigt man denn am häufigsten? Wahrscheinlich die TCP-Analyse, mit deren Hilfe man die gefürchteten Paketverluste und ihre Folgen erkennt (Retransmissions, Duplicate Acknowledgements, etc.). Und das kann Ethereal auch. Inzwischen ist die entsprechende Funktion (*Edit > Preferences > Protocols > TCP > Analyze TCP sequence numbers*) standardmäßig aktiviert. Findet Ethereal ein TCP-Problem, so wird es in eckigen Klammern der Info-Zeile des Pakets vorangestellt. Im Paket-Detail findet sich die Problembeschreibung unter *SEQ/ACK analysis*. Hier kann man natürlich wieder mit der rechten Maustaste ein Filter setzen. Hat man also einmal eine Retransmission gefunden, filtert man so schnell alle heraus. Ich habe meine Ethereal-Installation unter *View > Coloring Rules* so eingestellt, dass alle TCP-Probleme rot markiert werden. Auch an dieser Stelle gibt man im Übrigen nichts anderes ein, als einen Filter. Entspricht das Paket dem Filter, wird es entsprechend angemalt.

7. Ethereal und WLAN

Zum Schluss ein kleiner Exkurs in die Analyse von WLAN-Paketen auf der Luftschnittstelle. Zunächst sei bemerkt, dass es WLAN-Analyse immer nur gegen Aufpreis gibt. So auch bei Ethereal. Der Aufpreis besteht darin, dass man dafür um

Verdrängt Open Source traditionelle LAN-Analyse-Produkte? Ethereal produktiv einsetzen

eine Installation unter LINUX nicht herum kommt. Das ist im Allgemeinen nicht ganz ohne, da man Ethereal für LINUX nur in der Form von Quelldateien bekommt. Man benötigt also ein wenig Kenntnis über Compiler, Makefiles, und das Einbinden der benötigten Bibliotheken. Wer sich also die aktuelle Ethereal-Version selbst übersetzen möchte, dem empfehle ich, zuvor die neuste Version des GTK+, wie man sie unter ftp://ftp.gtk.org/pub/gtk/v2.4 bekommt, inkl. der Bibliotheken GLIB, PANGO und ATK zu installieren. Dazu kommt das Paket PKG-CONFIG und die LIBPCAP in der Version 7.2 oder höher. Nicht zuletzt benötigt man natürlich einen Treiber für die WLAN-Karte, der soweit gepatcht ist, dass er die MAC-Pakete (Beacons etc.) an die Capure-Engine übergibt.

Wer bereits den LINUX Kernel der Version 2.6.x einsetzt, hat mindestens für den Orinoco-Chipsatz den entsprechenden Treiber dabei. Daraus ergibt sich meine Empfehlung für den LINUX-Einsteiger: Besorgen Sie sich die neueste KNOPPIX-Installation von Klaus Knopper (http://www.knopper.net). Dabei handelt es sich um ein LINUX, das ohne vorherige Installation von einer CD gestartet und betrieben wird. Es enthält sowohl den korrekten Orinoco-Treiber als auch Ethereal. Um damit nun WLAN-Pakete aufzeichnen zu können, gehen Sie in den folgenden Schritten vor:

- Öffnen Sie zunächst ein Terminal-Fenster und geben Sie *su* ein. Ethereal kann nämlich auf die Schnittstellen nur zugreifen, wenn es unter dem User „root“ ausgeführt wird.

- Finden Sie heraus, unter welchem Namen Ihre WLAN-Karte erkannt wurde, indem Sie *iwpriv* eingeben. Suchen Sie die Schnittstelle heraus, bei der Sie unter *Available private ioctl* eine Zeile mit *monitor* finden. Nehmen wir an, es sei „ethX“. Dann aktivieren Sie die Schnittstelle mittels *ifconfig ethX up*

- Nun geben Sie *iwpriv ethX monitor 1 <ch>* ein, „<ch>“ steht für den Kanal, auf dem Sie messen wollen, bei IEEE 802.11b also eine Zahl zwischen 1 und 13.

- Starten Sie nun Ethereal über den Befehl *ethereal&*. In den „Capture options“ wählen Sie als Interface „ethX“ aus und *Update list of packets in real time.*

- Am Ende deaktivieren Sie den Monitor-Mode mittels *iwpriv ethX monitor 0 0*.

Wenn alles geklappt hat und auf dem eingestellten Kanal tatsächlich ein WLAN aktiv ist, sollten nun zahlreiche Beacon-Frames zu sehen sein. Falls nicht, können Sie während laufender Aufzeichnung mit *iwpriv* einen anderen Kanal wählen und so nach belegten WLAN suchen (zur Suche nach WLAN empfehle ich allerdings „kismet –c orinoco,ethX,orinocosource“).

Vielleicht haben Sie ja jetzt „Blut geleckt“ und richten sich eine dauerhafte LINUX-Installation auf Ihrem Rechner ein....

Studie des Monats

Wireless LAN Evaluierung

Arbeitsweise, Varianten, Schwachstellen, Planung, Installation

Anstatt im Report eine sowieso immer unvollständige und veraltete Marktübersicht zu bringen, werden in Kapitel 7 die wesentlichen Ausstattungsmerkmale von Access Points beschrieben und bewertet:

Architektur

Es gibt zwei grundsätzliche Bauformen für Access Points:
- Kompaktgeräte und
- modulare Geräte

Bei den modularen Geräten ist das Radioteil in der Regel auf eine PCMCIA- oder Mini-PCI-Karte ausgelagert. Der Vorteil dieser Bauformen liegt auf der Hand: das Radioteil kann schnell und problemlos ausgetauscht werden. Je nach Hersteller ist auf diese Weise sogar ein Technologiewechsel von 2,4 GHz nach 5 GHz möglich. Einige Produkte bieten sogar zwei oder mehr Slots, die parallel betrieben werden können und auf diese Weise den Gesamtdurchsatz in der Funkzelle vervielfachen. Aufgrund der mangelnden Kanalanzahl im 2,4-GHz-Band ist das natürlich nur bei 802.11a/h sinnvoll.
Der Nachteil modularer Geräte liegt in der oft sehr einfachen Transceiver- und Antennentechnik, die in den kleinen Karten untergebracht ist. Außerdem verbietet sich die Installation solcher Systeme an leicht zugänglichen Stellen, da die PCMCIA-Karte ohne großen Aufwand herausgezogen werden kann.

Montagemöglichkeit

Praktische alle Access Points sind als Standgeräte konzipiert und sollen offensichtlich als einzelnes Gerät einen Schreibtisch zieren. Die meisten dieser Access Points haben zusätzlich die Möglichkeit einer Wandmontage, was mit einigem Geschick natürlich auch eine Deckenmontage nicht ausschließt. Das auffällige Design widerspricht allerdings in der Regel einer unauffälligen Unterbringungsmöglichkeit.

Zu Geräten, bei denen die Anschlüsse im Fuß untergebracht sind und die dann nicht mehr stehen bleiben, soll hier auf einen Kommentar verzichtet werden.

Antenne

Kompakte Systeme sind meist mit einem

oder zwei Dipolen ausgestattet. Hier sollte man darauf achten, dass die Antennen in genügend viele Raumrichtungen gedreht werden können. Dipole sollten unabhängig von der Montagerichtung des Access Points stets senkrecht ausgerichtet werden.
Bei modularen Systemen muss man sich entweder mit der integrierten Antenne zufrieden geben oder auf externe Antennen zurrückgreifen.

Diversity-Antenne

Diversity-Systeme haben in der Regel deutlich erkennbar zwei Antennen. Diversity kann in Bereichen mit Interferenzen durch Mehrwegeausbreitung (Reflexionen) die Empfangssituation deutlich verbessern. Als Merkregel gilt: Je größer die Funkzelle, desto mehr Reflexionen.

externe Antennen

Externe Antennen kosten vor allem zusätzliches Geld. Kann aus betrieblichen Gründen (siehe Kapitel 9) nicht auf externe Antennen verzichtet werden, muss sichergestellt werden, dass diese an den Access Point angeschlossen werden können. Nicht alle Systeme unterstützen das.

Sendeleistung

Die Anpassung der Sendeleistung ist ein wesentlicher Konfigurations- und Planungsparameter. Zum einen ermöglicht er die Realisierung kleinerer Funkzellen und damit eine höhere Access-Point-Dichte in der Fläche. Zum anderen kann die Reduzierung der Sendeleistung aufgrund der Bedingungen der Regulierungsbehörden erforderlich werden, wenn externe Antennen mit hohem Antennengewinn angeschlossen werden (siehe Kapitel 4.1.4).

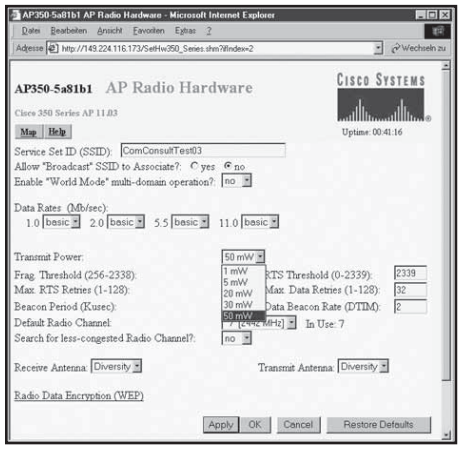


Abbildung 7.3: Anpassung der Sendeleistung

Außerdem können damit unnötige Reichweiten reduziert werden, um ein Netzwerk sicherer gegen Lauschangriffe von Außen zu machen.

Ethernet-Schnittstelle

Die 10-Mbit-Schnittstelle einiger 11b-Access Points ist passé. 11a- und 11g-Produkte sind alle mit einer 100-Mbit-Schnittstelle ausgestattet. Sollen an einem Access Point mehr als zwei Funkzellen gleichzeitig betrieben werden, sind sogar Gigabit oder getrennte Uplinks Pflicht.

Power over LAN

Unter dem Gesichtspunkt einer möglichst optimalen Unterbringung des Access Points, zum Beispiel oberhalb von Zwischendecken, kann Power over LAN die Installationskosten deutlich reduzieren. In wie weit daraus Folgeinvestitionen wie redundante Stromversorgung, Notstrom oder aktive Kühlung in den Verteilerräumen entstehen, muss im Einzelfall geprüft werden.

Die zugehörige Norm IEEE 802.3af (siehe [8]) ist allerdings noch nicht verabschiedet, befindet sich jedoch seit geraumer Zeit in einem stabilen Zustand. Die Betriebsspannung eines Access Points beträgt 36 V bis 57 V. Die Spannung an der Stromeinspeisung (Netzteil) beträgt 44 bis 57 V. Der maximale Spannungsabfall von 8 V stellt für die bei Ethernet über Kupfer

verwendeten Kabellängen kein Problem dar. Die Stromaufnahme beträgt maximal 350 mA. IEEE 802.3af legt ein Verfahren fest, das erkennt, ob ein Endgerät eine Stromversorgung über das Datenkabel unterstützt oder nicht. Dies schützt vor Beschädigungen bei einem Anschluss eines Geräts, das keine Stromversorgung über das Datenkabel erwartet und an einen Port angeschlossen wird, der eine solche Stromversorgung unterstützt.

IEEE 802.3af spezifiziert zwei unterschiedliche Alternativen für die Pin-Belegung zur Stromversorgung über das Datenkabel (siehe Tabelle 7.1):

- Alternative A nutzt die Pins 1, 2, 3 und 6, die stets auch zur eigentlichen Datenübertragung verwendet werden.
- Alternative B nutzt dagegen die „freien" Pins 4, 5, 7 und 8.

Beide Alternativen A und B können von einem Gerät zur Stromversorgung über das Media Dependent Interface (MDI) unterstützt werden. Der Standard verbietet jedoch die simultane Nutzung beider Alternativen auf einem Kabel. Für Alternative A sind zusätzlich zwei mögliche Polarisierungen spezifiziert (MDI-X und MDI). Alternative B kann bei Aufteilung eines 8-adrigen Kabels auf zwei Anschlüsse (Cable Sharing) nicht verwendet werden.

Pin	Alternative A MDI-X	Alternative A MDI	Alternative B
1	-Up	+Up	
2	-Up	+Up	
3	+Up	-Up	
4			+Up
5			+Up
6	+Up	-Up	
7			-Up
8			-Up

Tabelle 7.1: Pin-Belegungen zur Stromversorgung

Die Stromeinspeisung auf die Datenleitung kann entweder durch einen Access Switch des Distribution Systems oder durch ein so genanntes „Power Patch Panel" geschehen (siehe Abbildung 7.4). Vorteilhaft für die Stromversorgung mit einem Access Switch ist, dass keine zusätzlichen Geräte benötigt werden. Nachteilig sind die entstehenden Kosten, da diese Switches zumindest aktuell noch deutlich teuerer sind als konventionelle Switches. Die Entscheidung muss im Einzelfall getroffen werden. Zu beachten ist noch, dass nicht alle Herstellerlösungen zur Stromversorgung über Ethernet wirklich kompatibel zum aktuellen Draft von IEEE 802.3af sind. Es muss also stets verifiziert werden, ob Access Point und stromversorgender Switch bzw. Power Patch Panel tatsächlich zusammen passen.

Einige Produkte bieten auch eigene Koppelelemente an, um Strom zumindest auf den letzten Metern über das LAN-Kabel führen zu können.

DHCP

Das lokale System wahlweise mit einer festen IP-Adresse oder einer dynamischen Adresse über DHCP zu versorgen, ist mittlerweile Standard.

Im Gerät integrierte DHCP-Server sind natürlich in erster Linie für den Konsumermarkt gedacht, können aber auch bei der Anbindung kleiner Außerstellen hilfreich sein - insbesondere wenn das Gerät gleichzeitig als DSL-Router die Anbindung selbst übernimmt.

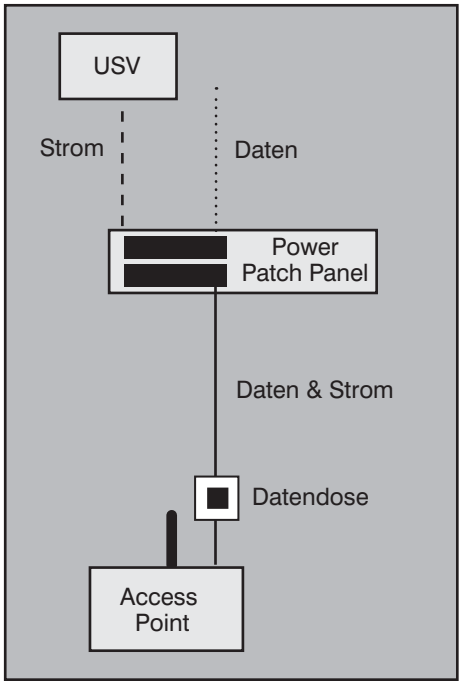


Abbildung 7.4: Anschluss eines Power Patch Panels

Routing

Systeme mit mehreren Ethernet-Schnittstellen und/oder mit integriertem DSL- oder ISDN-Router adressieren ebenfalls hauptsächlich den privaten Nutzer oder werden zur Anbindung kleiner Geschäftsstellen genutzt.

Zur Bewertung der Routing-Funktionalitäten ist im Wesentlichen zu beachten, in wie weit Routing-Regeln auch auf die internen Schnittstellen gebunden werden können. Nur wenn Routen auch nach innen zeigen können, ist das System für Standorte mit mehreren Subnetzen geeignet.

Firewall

Eine zusätzliche Firewall überfordert in der Regel die Systeme und bietet daher meist nur abgespeckte Funktionalitäten. Letztlich erzeugt dies jedoch nur ein sehr trügerisches Gefühl von Sicherheit und ersetzt keineswegs eine vollwertige Firewall oder wenigstes Personal Firewalls auf den Endsystemen.

Außerdem muss genau hinterfragt werden, wer vor wem geschützt werden soll: das Funk-LAN vor dem Internet oder das kabelgebundene LAN vor dem Funk-LAN.

Viele Access Point gestatten stattdessen die Verwaltung von Protokoll-Filtern. Meist kann lediglich auf das Ethernet-Protokoll gefiltert werden, zum Teil aber auch auf IP-Protokoll, TCP/UDP-Port und IP-Adresse.

802.11-Funktionen

Das Setzen von Thresholds für Fragmentierung und das RTS/CTS-Verfahren gehören zu den Minimalanforderungen, und zwar stufenlos und ohne Einschränkungen, dass beispielsweise der eine Wert größer sein muss als der andere.

Das individuelle Konfigurieren von Basic Rates kann im Einzelfall sinnvoll sein, wird aber in der Regel auch die Fehlersuche komplizieren.

Das Setzen eines „World Modus" ist für Firmen interessant, die Besucher aus anderen Regulierungszonen wie zum Beispiel den USA unterstützen müssen. Der Access Point informiert dabei den Client, dass er in Europa ist und hier andere Regulierungsbeschränkungen gelten. Dies muss allerdings auch vom Client unterstützt werden.

Sicherheit

WPA ist Pflicht. Die Upgradefähigkeit auf 802.11i sollte gefordert werden.

MAC-Filter können verwaltet werden, wenn einem langweilig ist - ein wirkliche Hilfe ist dies nicht.

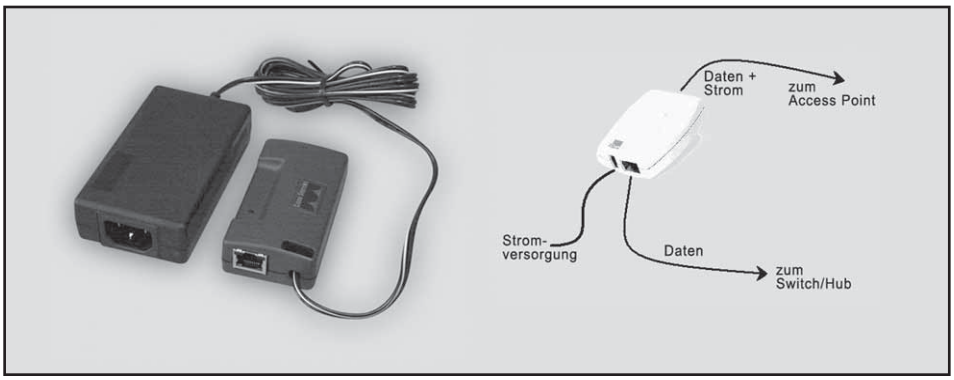


Abbildung 7.5: Koppelelemente von Cisco und 3Com

Wi-Fi Zertifikat

Auch wenn man auf die Interoperabilität mit anderen Herstellern verzichten kann, ein Wi-Fi Zertifikat gehört eigentlich zur Grundausstattung.

Management-Schnittstelle

Hier sind alle Möglichkeiten vertreten, die man sich denken kann: serielle Schnittstelle, USB oder nur LAN, Management über telnet, ssh, http oder SNMP, jeweils mit grafischer Oberfläche oder als CLI. Eine Web-Schnittstelle zumindest als zusätzliche Option scheint sich allgemein durchzusetzen. Bei diesem Sammelsurium sollte man auf folgende Anforderungen achten:

- Das Management über die Funkschnittstelle muss deaktiviert werden können.
- In öffentlichen Bereichen muss ebenfalls das Management über lokale Schnittstellen (seriell oder USB) deaktiviert werden können.
- Nur SNMP stellt eine zukünftige Integration in ein übergeordnetes Management und eine Eventüberwachung in Aussicht.
- SNMP muss in der Version 3 unterstützt werden.
- Je nach Organisation müssen benutzerspezifische Einschränkungen der Konfigurationsoberfläche realisiert werden. Das bedeutet entweder eine lokale Benutzerverwaltung oder besser die Rechtevergabe durch ein zentrales System, bei dem es sich in der Regel um einen RADIUS-Server handeln wird.
- Werden umfangreiche Konfigurationseinstellungen vorgenommen, ist es hilfreich, wenn man die Konfiguration per Download sichern kann.

Betriebsmodus

Neben ihrem standardmäßigen Betriebsmodus als Access Point können einige Produkte auch im so genannten „Repeater-Mode“ oder als „LAN-Bridge“ zusammen mit einem zweiten Access Point in einer Punkt-zu-Punkt-Verbindung oder sogar einer Punkt-zu-Multipunkt-Verbindung zur Kopplung von Ethernet-LAN-Segmenten eingesetzt werden. Neben diesen Umschaltfähigkeiten ihrer Standardgeräte vertreiben viele Hersteller auch dedizierte Geräte als „Wireless Bridge“ o.ä. zum expliziten Einsatz in solchen Sonderfällen.

Schwerpunktthema

Rahmenbedingungen und Kriterien für einen zukunftsorientierten WLAN-Einsatz

Fortsetzung von Seite 1

Dr. Jürgen Suppan ist Geschfätsführer der ComConsult Akademie und von ComConsult Research. Er zählt seit über 10 Jahren zu den anerkanntesten internationalen Experten auf dem Gebiet der Netzwerke und verteilten Systeme. Unter seiner Leitung wurden diverse Projekte unterschiedlichster Größen erfolgreich durchgeführt. Hohen Bekanntheitsgrad haben seine Veröffentlichungen und Analysen zur Nutzbarkeit neuer Technologien.

Trotzdem wirft gerade der Aspekt einer zukunftsorientierten WLAN-Installation, sprich die Entscheidung für das im wirtschaftlichen und technischen Sinne richtige

- Design
- die richtige WLAN-Variante
- das richtige Sicherheitskonzept
- das geeignete Betriebskonzept

eine Reihe wichtiger Fragen auf. Fehlentscheidungen unter falscher Einschätzung der zukünftigen Veränderungen können nicht nur zu einem Neudesign mit allen notwendigen Arbeiten zwingen, sie würden vor allem auch signifikante Unterbrechungszeiten nach sich ziehen.

Der folgende Artikel geht auf die Eckpunkte einer zukunftsorientierten WLAN-Umsetzung ein, indem er wichtige Grundsatzentscheidungen beleuchtet und mögliche Alternativen anspricht. Die Berücksichtigung dieser Eckpunkte ist Voraussetzung für einen langfristigen Erfolg eines WLAN-Projekts. Dabei spielen insbesondere die Rückwärtskompatibilität zu den älteren und die Vorwärtskompatibilität zu den neuen Standards, hier speziell IEEE 802.11n, eine große Rolle.

Speziell der langfristige Aspekt wird im Markt häufig vernachlässigt, unter anderem auch deshalb, weil einzelne der traditionellen LAN-Hersteller die Einführung gerade professioneller WLANs systematisch behindern und verzögern. Die Ursache ist hier im Bereich der hohen Kosteneinsparpotenziale dieser Technologie zu sehen. Einige Hersteller fahren deshalb die Strategie, die Marktumsetzung professioneller WLAN-Technik möglichst um ein oder zwei Jahre zu verzögern. Dies ist u.a. an der Verfügbarkeit der IEEE 802.11a/h-Technologie sehr gut zu beobachten. Für den Kunden gilt, dass er sich auf diese Strategie nicht einlassen sollte, es gibt genügend seriöse Anbieter aller wichtigen WLAN-Technologien. Und es gibt eindeutig Hersteller, die wichtige neue Standards schneller umsetzen als andere (siehe: Einführung von 11a/h, Umsetzung von 11i). Im Vordergrund sollte immer die gegebene Bedarfssituation des Kunden stehen. Wenn ein Hersteller WLAN-Technologie nicht engagiert betreibt und immer nur mit großer Verzögerung wichtige Neuerungen bereitstellt, dann sollte auf einen anderen Hersteller ausgewichen werden.

Auch der Kostenaspekt ist dabei nicht zu vernachlässigen. Es empfiehlt sich dringend, gerade bei WLAN-Technologie nicht schon mit einem von vornherein gesetzten Hersteller in die Planung einzusteigen. Die Kostenunterschiede, gerade im Bereich der Access-Points, die in Summe die Gesamtkosten prägen, kann bis zu 50% betragen, ohne dass funktionale oder sonstige technische Vorteile zu erkennen sind (der Vergleich bezieht sich rein auf professionell nutzbare Produkte und bezieht Konsumer-Produkte nicht ein). Hier ist der Weg, zuerst herstellerneutral die gewünschten Eigenschaften zu definieren und dann nach dem wirtschaftlich optimalen Hersteller zu suchen, der eindeutig bessere Weg. Vorsicht ist bei kleineren Newcomern angebracht, hier sollte vor größeren Investitionen der finanzielle Background und die Zukunftssicherheit des Anbieters geprüft werden.

Bei keiner Netzwerkplanung sollte dabei außer Acht gelassen werden, dass die Kombination aus der kontinuierlichen Weiterentwicklung von WLANs und die permanent wachsende Zahl strategisch wichtiger Endgeräte mit integrierter WLAN-Fähigkeit mit hoher Wahrscheinlichkeit die WLAN-Technologie in den nächsten Jahren massiv puschen werden. Über einen Zeitraum von 5 Jahren werden WLANs zum unverzichtbaren Bestandteil jedes Unternehmensnetzwerks werden.

Für viele Neubauprojekte wird nach Verabschiedung des IEEE 802.11i-Standards die Frage nach einer weitestgehend kabellosen oder gezielt gemischten Vernetzung (mit starker Verringerung des Kabelanteils) entstehen. Zurzeit kann man nach Untersuchungen von ComConsult Research davon ausgehen, dass sich die Kosten der Vernetzung für ein Neubauprojekt dabei um ca. 40% im Schnitt senken lassen (siehe [1]).

Im Folgenden wird auf eine Auswahl der wichtigen Eckpunkte für ein Wireless-Projekt eingegangen. Die Liste ist ggf. nicht vollständig, vermittelt aber ein gutes Bild der aktuellen Entscheidungslage.

1. Die Zukunftssicherheit einer WLAN-Installation:

WLAN-Technik entwickelt sich in mehrfacher Hinsicht weiter. Innerhalb der nächsten Jahre wird es massive Änderungen dieser Technologie geben. Trotzdem ist eine aufwärtskompatible und somit investitionssichernde Umsetzung möglich, wenn die kommenden Änderungen berücksichtigt werden. Herausragende Änderungen sind dabei:

- die Bandbreite von Wireless LANs wird in den Gigabit-Bereich steigen, die aktuellen Arbeiten am IEEE 802.11n-Standard sind der Einstieg in diese Entwicklung. Innerhalb der nächsten 2 Jahre werden mindestens 200 bis 400 Mbit/s erreicht. Generell gilt dabei, dass nur genormte Varianten zum Einsatz kommen sollten. Das Angebot nicht genormter Varianten, so wie es gerade wieder im Vorgriff auf IEEE

802.11n erfolgt, ist grundsätzlich als unseriös zu betrachten und führt nur in eine Herstellerbindung (sowohl auf der Seite der Access Points als auch auf der Seite der Client-Adapter)

- die Umsetzung anwendungsspezifischer Service-Qualitäten wird weiter zunehmen. Mindestens Quality of Service und VLAN-Techniken werden dabei weiter entwickelt werden. Aber auch eine gezielte Steuerung der verfügbaren Bandbreite mit besonderer Unterstützung kritischer Applikationen wird Stand der Technik werden. Treiber dieser Entwicklung wird vor allem IP-Telefonie über WLAN sein. ComConsult Research spricht dieser Technik durchaus das Potenzial zu, auf einen Zeitraum von 5 Jahren DECT abzulösen

umso intensiver stellen, sind:

- Soll eine komplette Sicherheits-Infrastruktur mit Anmeldeserver etc. aufgebaut werden oder soll Sicherheit nur zwischen Client und Access Point über Preshared Keys umgesetzt werden?

- Soll für den Wireless-Bereich eine separate Sicherheitslösung gefahren werden oder wird eine alles übergreifende Gesamtlösung angestrebt?

- Wie wird generell der Wireless-Bereich mit den bestehenden kabelgebundenen Netzwerken verbunden? Bildet das Wireless-Netzwerk eine große Layer-2-Domäne, die an einem zentralen Punkt verbunden wird? Realisiert das Wireless-Netzwerk eine Layer-3-strukturierte Netzwerklösung mit zentralem Übergang? Besteht das WLAN aus Layer-2-Zellen, die jeweils einzeln als IP-Subnetz an den bestehenden Backbone angeschlossen werden?

- Was bedeutet der neue IEEE 802.11-Standard für die Praxis, wie wird er eingesetzt, hat er Einfluss auf die Performance, wie passt er in eine übergeordnete Sicherheits-Infrastruktur?

Generell geht der Trend zur Bildung so genannter Sicherheitszonen. Ein Netzwerk, auch wenn es Layer-3-strukturiert ist, wird dabei in getrennte Sicherheitszonen mit kontrollierten Übergangspunkten unterteilt. Hintergrund ist ein leichteres Security-Operating und eine verbesserte Reaktionsmöglichkeit auf erfolgreiche Attacken, Würmer, Viren etc. Im Endeffekt unterstellt man, dass es den vollständigen Schutz nicht gibt und dass man im Falle eines Angriffs Teile der vorhandenen Netzwerk-Infrastruktur bewusst isolieren wird. Sei es zum Schutz oder zur Isolierung des verschmutzten Netzwerkbereichs.

In diesem Sinne wäre eine einfache Layer-2-Anbindung von Wireless-Zellen an bestehende Etagen- oder Core-Switches in Frage zu stellen. Hier wird keinerlei Möglichkeit der Kontrolle oder des Einflusses auf sicherheitsrelevante Vorgänge geschaffen.

Allerdings ist in jedem Fall zu berücksichtigen, dass 802.11i für Unternehmensnetze zwingend die Umsetzung des LAN-Sicherheitsstandards 802.1X fordert (die „kleine“ Lösung mit Preshared Keys ist ausschließlich für den Homebereich vorgesehen). Mit 802.1X hat man aber die reale Chance, alle mobilen Geräte der gleichen Sicherheitspolicy zu unterwerfen - egal ob sie über Kabel oder Funk angebunden sind.

Je nach Größe der Wireless-Installation kann die Sicherheitslösung sehr umfangreich werden. Dabei gilt die Regel, dass je größer die Installation desto mehr der Weg in eine umfassende Sicherheitslösung gesucht werden sollte, die alle vorhandenen Kommunikationsbereiche abdeckt.

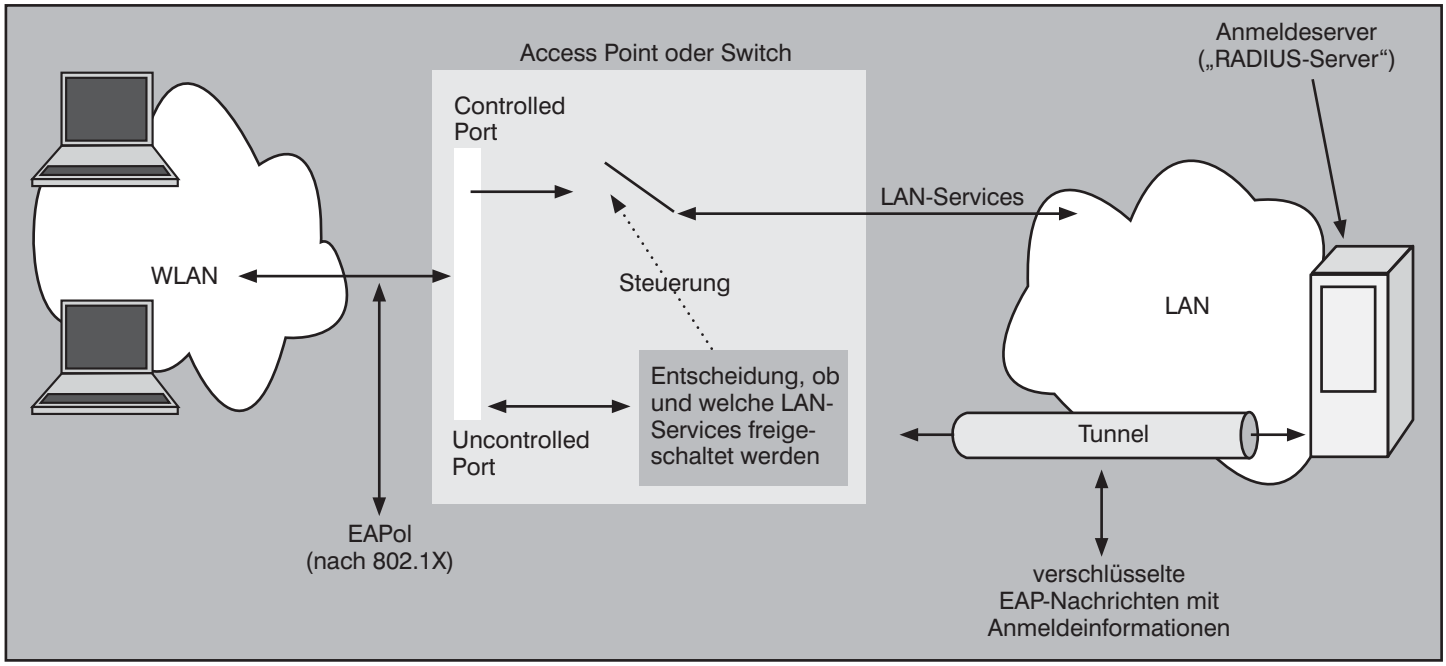


Abbildung 1: Sicherheitsinfrastruktur nach IEEE 802.11i

2. Umsetzung des neuen Sicherheitsstandards IEEE 802.11i:

Endlich ist der lange erwartete Sicherheitsstandard für Wireless-Netzwerke verabschiedet worden. Er löst nicht nur die bestehenden Sicherheitsprobleme, er macht aus WLANs die sicherste im Moment existierende Netzwerktechnik. Allerdings setzt der höchste Grad an Sicherheit eine Radius-Infrastruktur voraus, eine eingeschränkte Realisierung über Preshared-Keys unterliegt weiter dem Risiko von Dictionary-Attacken. Aus diesem Grund sieht der Standard Preshared-Keys auch nur für den privaten Gebrauch vor. Die zentralen Grundfragen, die sich damit

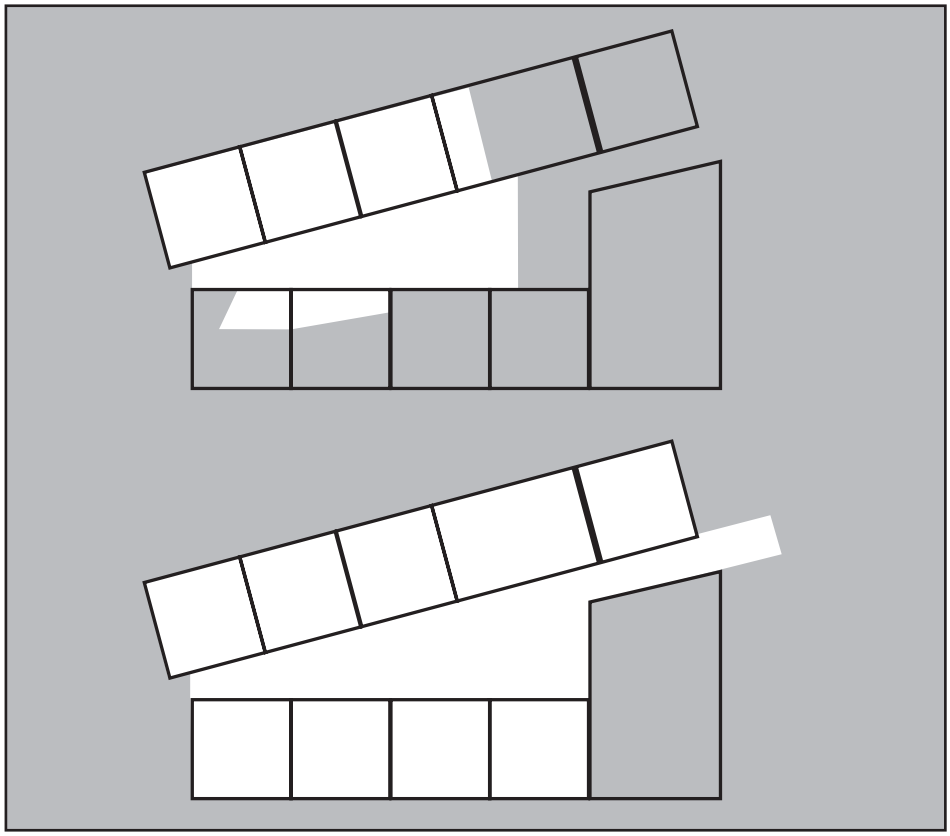


Abbildung 2: Reichweite von bei 802.11a mit 30 mW (oben) und 200 mW (unten)

3. Ist IEEE 802.11a einsatzbereit?

Mittlerweile werden IEEE 802.11a Produkte von vielen Herstellern angeboten. Die Vorteile liegen auf der Hand: keine Überschneidung mit 2,4 GHz-Anwendungen und eine deutlich höhere Kanalzahl, so dass einzelnen Anwendungen eigene Frequenzen zugewiesen werden können. Mit der Freigabe des Centrino-Pro/Wireless ABG-Chipsets durch Intel noch in diesem Monat wird der Weg für die generelle Integration von 11a in Notebooks eingeschlagen. Die geringen Mehrkosten von ca. 4 Dollar gegenüber den bisherigen Chips werden dafür sorgen, dass bereits in kurzer Zeit Notebooks generell mit a/b/g-Fähigkeit ausgeliefert werden.

Aber bei näherer Betrachtung unterscheiden sich gerade 11a-Produkte erheblich. Nach wie vor gibt es viele 30mW-Produkte, die schlicht unbenutzbar sind. Ihre Reichweite ist so gering, dass sie häufig schon an der ersten Wand scheitern. 30 mW sind für 5 GHz eindeutig zu wenig. Die unprofessionelle und wenig überlegte Auflage der RegTP, die Überschneidung mit bestehenden 5 GHz-Anwendungen verhindern soll, behindert hier den Markt (zudem zeigen Messungen von Com-Consult, die die Einwirkung von Flugzeugradar geprüft haben, dass die Auflagen der RegTP nicht wirklich nachvollziehbar sind).

Die RegTP verlangt in Anlehnung an ETSI Transmit Power Control und Dynamic Frequency/Channel Selection. Dies wird im Markt häufig mit der Bezeichnung 11h gleichgesetzt, ist es aber technisch nicht. Leider hat die RegTP versäumt, eine Art Abnahme oder Freigabe zu schaffen. Für alle Hersteller, die heute DFS und TPC anbieten, entsteht damit das Problem, dass sie nicht wissen, ob ihr Produkt den Auflagen der RegTP entspricht. Viele haben so reagiert, dass sie DFS und TPC anbieten, aber bei 30 mW bleiben, um nicht gegen unklare Teile der RegTP-/ETSI-Bestimmungen zu verstoßen (vielleicht sollten die Damen und Herren der RegTP und von ETSI mal zur Abwechselung im wirklichen Leben arbeiten, damit dieser Unfug aufhört). Auch für den neuen Intel-Centrino-Chipsatz ist bisher nicht bekannt, ob er mit 30mW oder mit 200mW senden wird.

Bei der Auswahl von 11a-Produkten muss also dediziert geprüft werden, ob die 200mW umgesetzt werden, und zwar auf Access-Point und Client-Seite. Nur die 200mW-Lösung ist für einen professionellen Einsatz geeignet.

Der Normungstrend ist an dieser Stelle eindeutig. Die Normung geht für die Zukunft klar in den 5 GHz-Bereich. Im Sinne einer zukunftsorientierten Netzwerk-Planung wäre der Wechsel in den 5-GHz-Bereich also klar zu bevorzugen. Hin-

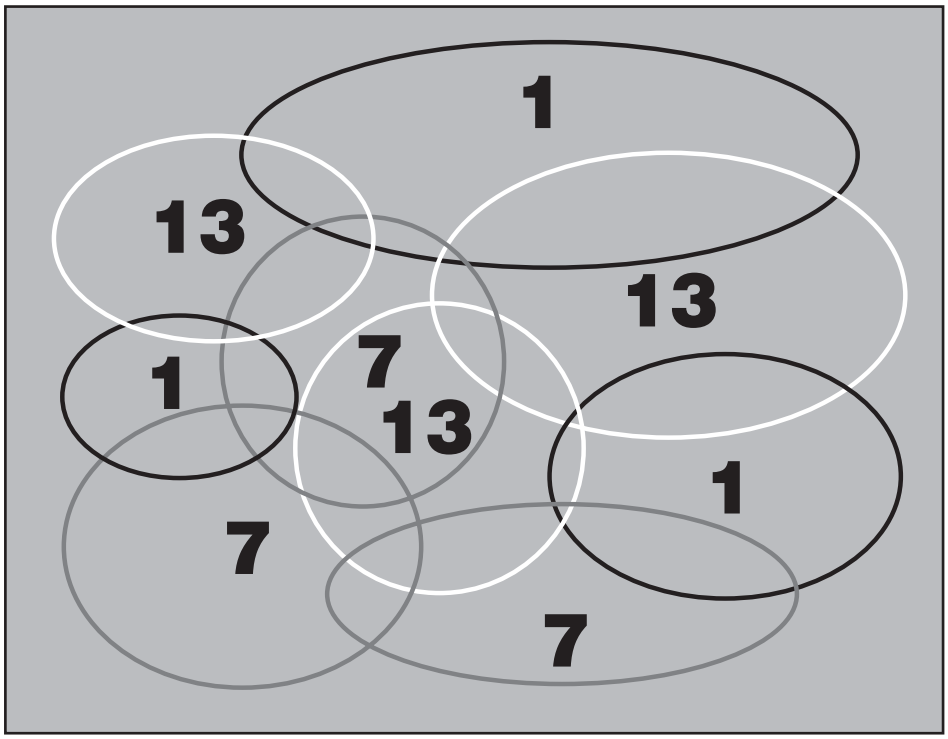


Abbildung 3: Ein überlappungsfreies Design mit nur drei Kanälen wird in der Realität nicht möglich sein

zu kommt, dass mit der Nutzung eines IEEE a,b,g-Acess-Points eine Lösung geschaffen wird, bei der b und g die Rückwärts-Kompatibilität sichern, die aber bei vorhandenen 11b-Teilnehmern immer mit Nachteilen für 11g-Teilnehmern verbunden sein wird. In diesem Sinne wird 11g zunehmend auf die Umsetzung von Rückwärtskompatibilität reduziert werden. 11a/h realisiert dann den zukunftsorientierten Leistungs-Anwendungsbereich.

Die zentrale und sehr spannende Frage beim Einsatz von 11a ist die konstruktive Nutzung der hohen Kanalzahl. Schon auf den ersten Blick drängen sich Gedanken, wie die exklusive Zuordnung von Kanälen zu Anwendungen auf (zum Beispiel der Voice-Kanal). QoS-Prioritäten würden dann auf Kanäle abgebildet. Leider ist dies nicht so trivial wie auf den ersten Blick anzunehmen. Das Grundproblem liegt in der dynamischen Änderung von Kanalbelegungen, so wie es die RegTP fordert. Zurzeit gibt es kein Produkt, das eine QoS-Kanalzuordnung dynamisch beibehält.

Es ist aber zu erwarten, dass sich die 11a-Produkte gerade im Bereich der optimalen Ausnutzung der angebotenen Kanäle deutlich fortentwickeln werden.

4. Interoperabilität zwischen den Wireless-Standards

Jede Wireless-Installation muss sich an den vorhandenen Teilnehmern orientieren. Diese bieten zunehmend einen Mix aus 11b und 11g-Teilnehmern, 11a-Teilnehmer werden diese Runde in Kürze bereichern. Somit entsteht die Aufgabe, in einer Funkzelle mehrere Standards zu unterstützen. Wie schon zuvor ausgeführt ist das nicht optimal, da die Rückwärtskompatibilität, egal wie sie umgesetzt wird, immer mit einer Benachteiligung der hohen Datenraten erkauft wird. Aus diesem Grund sollte eine moderne Wireless-Lösung immer zweigeteilt sein. Es sollte mindestens einen rückwärtskompatiblen Bereich und einen Vollleistungsbereich geben. Es ist offensichtlich, dass dies mit drei Kanälen im 2,4 GHz-Bereich nicht geht. Saubere Rückwärtskompatibilität ohne Beeinträchtigung geht nur mit einer Kombination aus 2,4 GHz und 5 GHz. 2,4 GHz sammelt die „alten“ Endgeräte, 5 GHz ist der Weg in die Zukunft.

5. Redundanz

Je höher die Flächendeckung von WLANs ist, je wichtiger die Anwendung, desto mehr stellt sich die Frage, was beim Ausfall eines Access Points passiert. Man stelle sich eine Transport-Steuerung vor, eine Vernetzung im Bergbau, ein automatisiertes Hochregallager oder ein Krankenhaus um sich darüber im Klaren zu sein, dass auch und gerade im WLAN-Bereich eine Redundanz-Lösung zwingend erforderlich ist. Speziell im Bereich der Optimierung von Arbeitsabläufen wird bedingt durch den Einsatz entsprechender Endgeräte zunehmend auf WLAN-Technik gesetzt. Wenn aber wichtige Arbeitsabläufe von WLANs abhängen, muss die Lösung ausfallsicher sein.

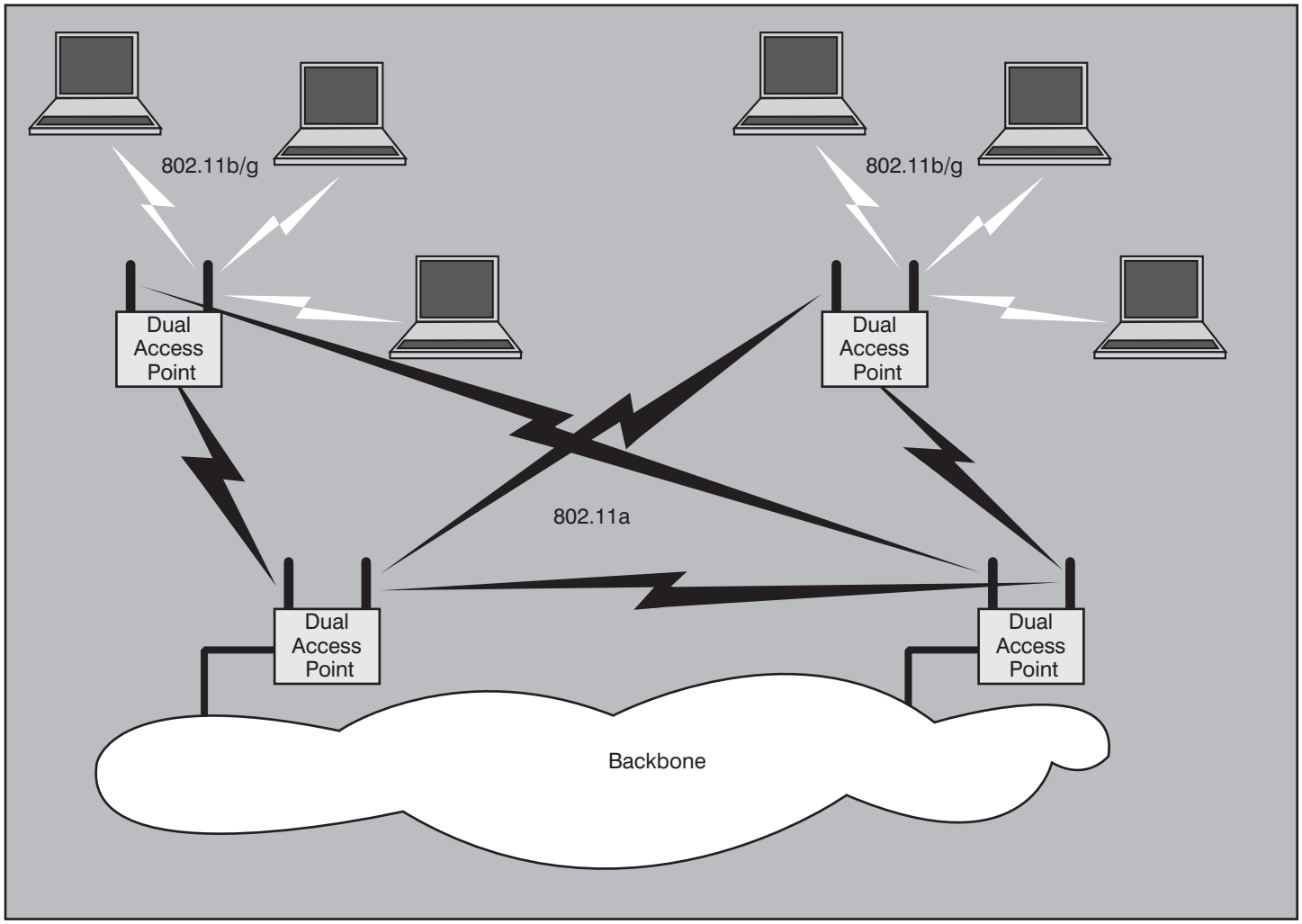


Abbildung 4: Redundante Netzwerkstrukturen mit Siemens Access Points

Das Problem liegt hier in der Flächendeckung bei gleichzeitiger Vermeidung von Interkanal-Interferenzen. Im Endeffekt bedeutet Redundanz immer, dass ein „Reserve"-Access-Point existieren muss. Die einfachste Lösung wäre natürlich immer ein Paar von Access-Punkten zu installieren, einen der operabel ist, einen der ohne eingeschaltetes Funkteil im standby steht. Dies wird angesichts der damit verbundenen Kosten nicht jeder wollen. Ist der Reserve-Access-Point jedoch auch voll operabel, so stellt sich sofort die Frage wie er ohne Interferenzen die Fläche eines anderen Access-Points abdecken kann und

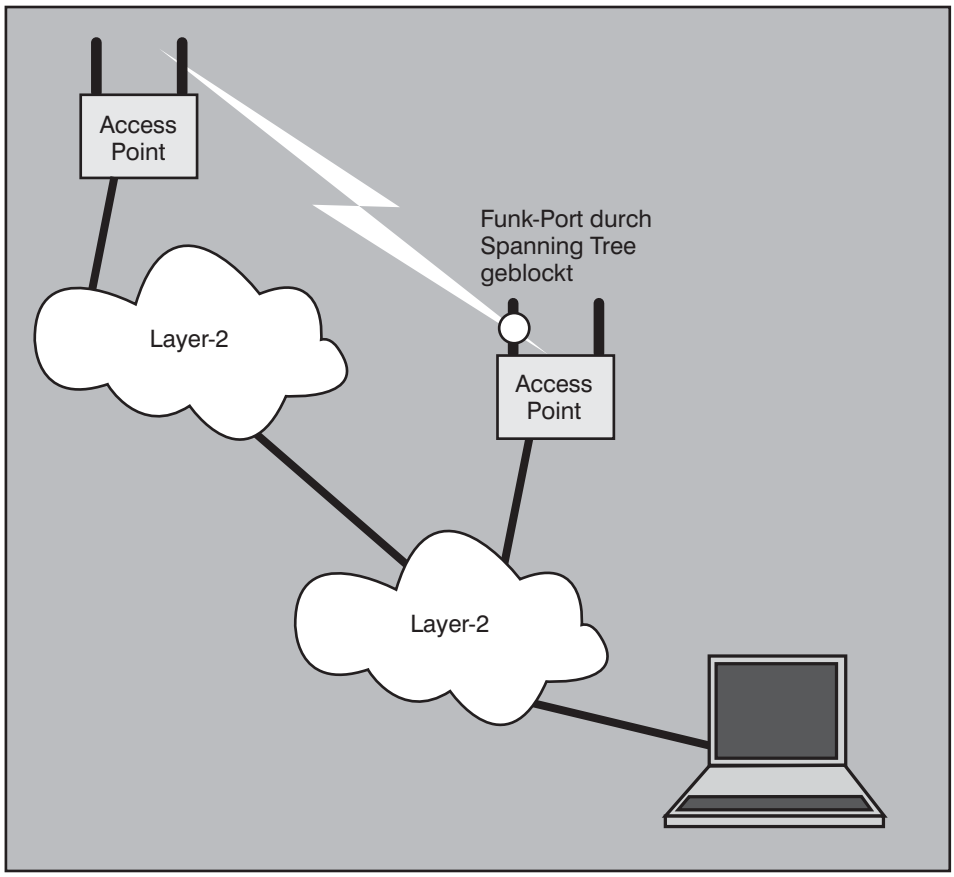


Abbildung 5: Redundante Funk-Kabel-Struktur

was nach dem Ausfall mit der erhöhten Last für diesen Access-Point passiert. In der Praxis wird man deshalb bei 11b/g auf ein Design mehrerer sich überlappender Zellen zurückgreifen, so dass sich beim Ausfall die Last auf mehrere „Reserve"-Access-Points verteilt. Damit steigen aber je nach Situation die Interferenzen an. Messungen von ComConsult-Research zeigen, dass dabei mit Verlusten zwischen 10% und 90% gerechnet werden muss.

Spannend sind auch weitergehende Konzepte, so wie sie zum Beispiel Siemens vorgestellt hat, die das Spanning-Tree-Protokoll zwischen den Access Points einsetzen.

Es ist aber offensichtlich, dass eine Mehrfachüberlappung im Bereich 11b/g nicht optimal ist. Auch die denkbare Störung durch andere 2,4GHz-Technologien ist für Anwendungen, die eine hohe Verfügbarkeit erfordern, nicht sinnvoll. Von daher ist gerade für Redundanzlösungen auf Dauer mit Lösungen im 5-GHz-Bereich zu rechnen. Hier kann mit einer Flächenabdeckung durch verschiedene Access-Points durch überlappungsfreie Kanäle gearbeitet werden. Denkbar und zu empfehlen ist auch, dabei so etwas wie feste Reserve-Kanäle zu schaffen.

Einen Sonderfall stellen Produktionsumgebungen dar. Naturgemäß sprechen wir hier über Spezialprodukte, die noch andere Anforderungen erfüllen müssen, die typisch für dieses Umfeld sind (stabile Stromversorgung, Feuchtigkeit, Vibration, Stoß, Temperatur).

Als Fazit für diesen Bereich bleibt festzustellen, dass die Schaffung von Redundanz mit 11b oder 11g nicht trivial ist und bei der Planung besonders berücksichtigt werden muss. Im Endeffekt kann eine wirklich saubere Redundanz-Lösung nur mit 802.11a/h geschaffen werden.

6. Planungsmethode

Die Planung eines Wireless-Netzwerks umfasst:

- Die Festlegung der Funkzellen in Lage und Ausdehnung inklusive der Zuweisung von Frequenzen und QoS-Paramtern an die Zellen
- Die Planung der Verbindung der Funkzellen untereinander
- Die Planung der Verbindung des WLAN mit dem Kabelgebundenen LAN oder einer anderen Infrastruktur

In jedem Fall ist das Ergebnis der Planung immer ein schriftliches Dokument. Da die Ausbreitung der Funkwellen von der gegebenen Umgebung abhängig ist (zum Beispiel also von der Zahl und vom Ort von Metallschränken, Flippcharts, Aquarien, großen Blumen, Metall-Regalsystemen abhängt) und sich diese Umgebung im Laufe der Zeit ändern kann, muss u.a. aus gewährleistungstechnischer Sicht die Planung dokumentiert werden. Üblich ist auch, mit einer Planungsreserve zu arbeiten, um diese unvorhersehbaren Änderungen zu kompensieren. Auch diese Planungsreserve sollte dokumentiert werden, ggf. auch grafisch in die Layout-Pläne übernommen werden.

Gerade die funktechnische Planung der Funkzellen wird immer mehr durch entsprechende Produkte unterstützt. Waren dies am Anfang noch sehr triviale Produkte, die sehr plump einfach nur die Signalausbreitungs-Formeln umgesetzt haben, so werden diese Produkte immer besser und damit für den Einsatz in der Praxis tauglicher (siehe zum Beispiel AirMagnet).

Bei der Planung der Zellenausdehnung sollte immer die Frage gestellt werden, mit welcher Anzahl und mit welchem Typ von Teilnehmern in Zukunft im Versorgungsbereich der Funkzelle zu rechnen ist. Dabei sollte die Versorgung pro Teilnehmer in der Zelle ausgerechnet werden, um zu prüfen, ob die Anforderungen der Teilnehmer erfüllt werden.

Je nach Einsatzbereich kann eine WLAN-Planung sehr aufwändig werden. Welche Planungsmethoden gibt es? Wie wichtig sind einzuplanende Zellüberlappungen? Was bedeutet Capacity Planning? Was leisten die neu auf den Markt gekommenen Planungstools? Wie kann der Planer für seine Planung Gewährleistung geben?

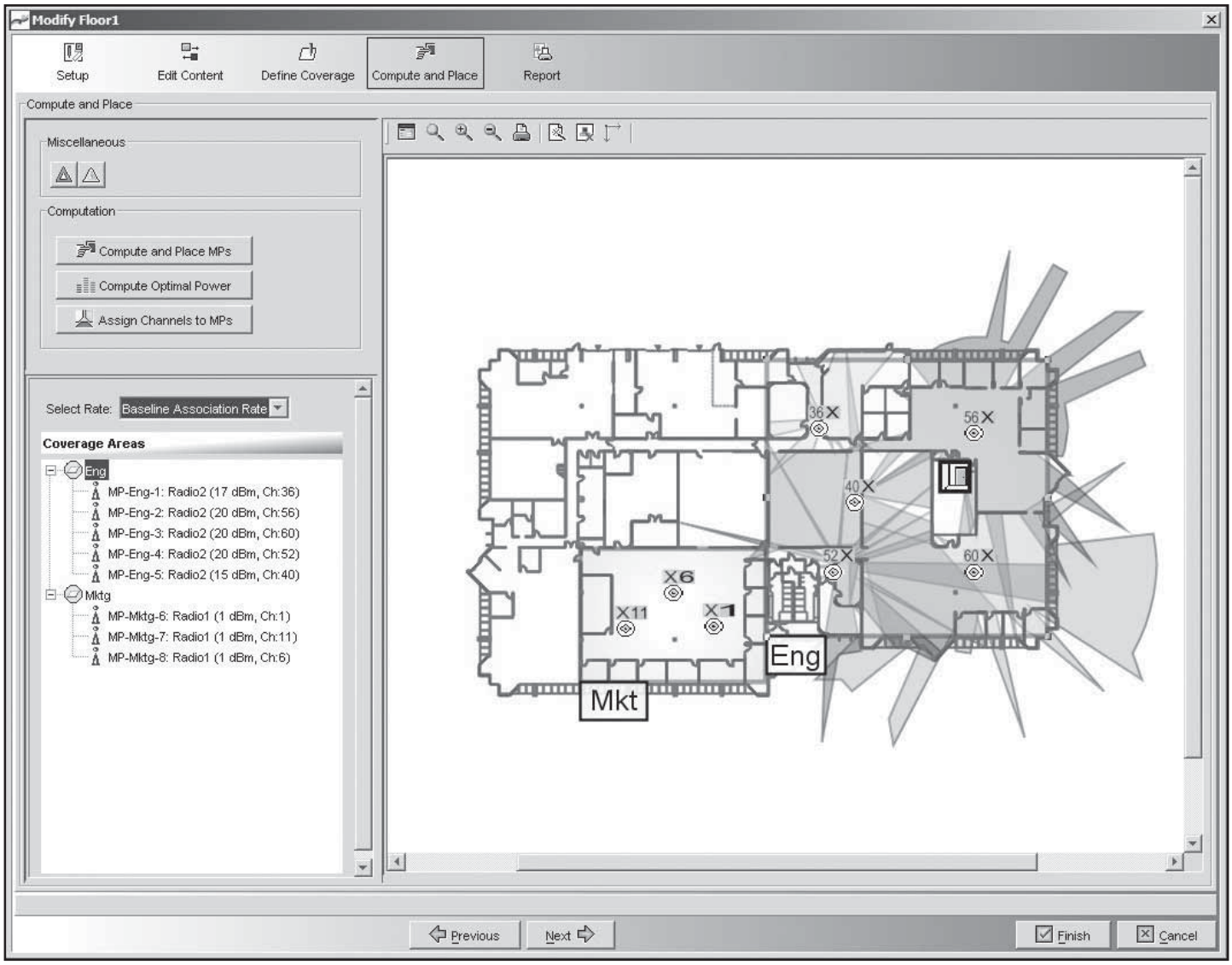


Abbildung 6: Site Survey Tool Air

Welche Tücken sind dabei zu beachten? Wie sieht eine korrekte Abnahme aus? Warum ist diese nicht trivial?

7. Art der Teilnehmer

Eine der Kernfragen der nächsten Jahre ist, welcher Typ von Teilnehmern in welcher Anzahl zu erwarten ist. Wir können mindestens von folgenden Endgerätetypen ausgehen:

- Notebooks: werden in Zukunft zu über 90% ein WLAN-Interface haben, dabei wird 11g vorerst dominieren, später wird verstärkt 11a hinzu kommen
- Desktops: werden häufig mit nicht geeigneten Adaptern ausgeliefert. Der Adapter sollte eine externe Antenne unterstützen. Bei Nachrüstung sollte ein a/b/g-Adapter mit externer Antenne gewählt werden, der bei 11a mit 200 mW arbeitet
- PDA: werden zunehmend mit WLAN-Integration ausgeliefert, die Ausstattungsquote wird auf über 90% ansteigen. Es dominiert auch noch auf längere Zeit 11b. Kernproblem für diese Geräte bleibt der hohe Stromverbrauch von Wireless
- Handys: werden ab 2005 zunehmend mit WLAN-Technik ausgestattet werden, dabei wird dann auch Voice over WLAN zur Nutzung in Hot-Spots unterstützt werden. Entsprechende Geräte sind bereits in der Entwicklung und werden von den IP-Telefonie-Herstellern gefördert
- Spezialgeräte: Scanner, serielle Schnittstellen, im Prinzip alle bisherigen Schnittstellen der Produktions- und Steuertechnik eignen sich zur Umsetzung auf WLANs. Hier dominiert zur Zeit noch 11b, da viele dieser Geräte keine hohen Bandbreiten benötigen, ist noch für längere Zeit damit zu rechnen, dass 11b der dominante Standard bleiben wird. Spannend ist bei diesen Geräten die Unterstützung von 11i - ohne 11i bleibt ein gravierendes Sicherheitsloch!! Die meisten Hersteller ignorieren zurzeit diesen Punkt. Innerhalb einer Planung sollte dies unbedingt beachtet werden, da sonst Angreifer, die die Adressen von Spezialgeräten spoofen freien Zugang zum Netzwerk erhalten.

Neben dem Typ der Teilnehmer ist die Frage nach deren Leistungsanforderungen zu stellen. Wie auch sonst in LAN-Planungen üblich werden diese Leistungsanforderung unterteilt in:

- Bandbreitenbedarf
- Garantierte Mindestbandbreite
- Verfügbarkeitsanforderung

- Delay/Zugangszeitanforderung
- Laufzeitanforderung
- Maximal zulässige Packet-Loss-Rate
- Mobilität

Als typisch für die Umsetzung dieser Leistungsanforderungen kann der Bereich der IP-Telefonie angesehen werden. Von vielen vielleicht noch als exotisch betrachtet, wird sich Voice over WLAN mit der Ausbreitung von IP-Telefonie schnell zum Standard entwickeln. Die Kernfragen, die sich aus diesen Leistungsanforderungen ergeben, lauten:

- Einsatz von Bandbreiten-Management
- Einsatz von Quality of Service
- Mobility-/Roaming-Umsetzung

Aus heutiger Sicht wird die Nutzung von Quality of Service für Wireless LANs nicht zu vermeiden sein. Solange bereits ein einzelner Teilnehmer eine Zelle monopolisieren kann, müssen Teilnehmer, die eine garantierte Mindestbandbreite und eine garantierte Zugangszeit benötigen, durch Quality of Service geschützt werden. Trotzdem sollte der Einsatz von QoS auf den WLAN-Bereich beschränlt bleiben und nicht aufs LAN ausgedehnt werden, da er dort unnötig ist und nur den Betriebs- und Analyseaufwand erhöht.

Sowohl bei Voice als auch bei den Spezialanwendungen stellt sich gerade in der Planung die Frage der Mobilität. Darunter wird ein sich bewegender Teilnehmer mit permanenter Übertragung auch während der Übertragung verstanden. Da die Funkzellen eines WLAN relativ klein sind, kommt es bei einer Bewegung unvermeidlich zum Wechsel der Funkzelle. Diesen Vorgang nennt man Roaming. Roaming erfordert ein Handover-Protokoll und einen zeitlich genau definierten Wechsel zwischen den Zellen, die so genannte Handover-Zeit. Dazu später mehr.

Neben dem reinen Problem des funktechnischen Wechselns in eine andere Zelle ist mit jedem Wechsel auch eine Sicherheitsfrage verbunden. Auf keinen Fall darf durch einen Zellwechsel eine Sicherheitslücke entstehen.

8. Roaming

Roaming wird in 3 bis 5 Jahren elementarer Bestandteil jeder WLAN-Realisierung sein. Zu viele neue Endgeräte kommen auf den Markt, die mobil sind und im laufenden Betrieb den Zellwechsel erfordern werden. Das Problem Roaming lässt sich nicht auf die Fähigkeit zum Zellwechsel reduzieren. Roaming erfordert ein Handover-Protokoll zwischen Access-Points, das im Standard IEEE 802.11f festgelegt ist. Die meisten Hersteller unterstützen als kleinsten gemeinsamen Nenner dieses Handover-Verfahren. Doch die wirklichen Probleme liegen einerseits im Bereich der Handover-Zeiten und andererseits in den mit dem Handover verbundenen Sicherheits-Risiken. Der gerade verabschiedete IEEE 802.11i-Standard schließt diese Sicherheitslücke und vermeidet, dass sich ein Client beim Wechsel der Zelle erneut beim Radius-Server anmelden muss. Wird allerdings dieser Standard nicht genutzt, kann Roaming schnell zu einem Angriff missbraucht werden.

Bei den Handover-Zeiten muss leider festgestellt werden, dass über 90% der von uns vermessenen Produkte die für einen unterbrechungsfreien Betrieb notwendigen Handover-Zeiten nicht eingehalten haben. Die Abweichungen von den Angaben, die die Hersteller zuvor gemacht haben und von den tatsächlich gemessenen Werten lagen bei mehreren hundert Prozent. Eine weitere Kernfrage des Hand-

overs ist die der Planung als Layer-2- oder als Layer-3-Struktur. Dabei besteht kein Zweifel, dass WLANs auf Dauer Layer-3-strukturiert werden müssen. Leider steigt damit die Handover-Zeit zurzeit noch massiv an. Auch ist anzumerken, dass der Bereich des Layer-3-Roamings zusätzliche Technologien benötigt und die Entwicklung in diesem Bereich noch nicht abgeschlossen ist (siehe Mobile-IP).

In der Praxis werden sich die Handover-Zeiten in Zukunft an den Anforderungen der Telefonie orientieren, eine Orientierung an einer unterbrechungsfreien TCP-Übertragung wird nicht ausreichen. Damit müsste der Handover im Sinne der vollständigen Wiederherstellung der Kommunikationsfähigkeit im zweistelligen Millisekundenbereich stattfinden.

9. Professioneller Betrieb

Mit der zunehmenden Zahl der WLAN-Teilnehmer muss ein WLAN-Betrieb als Teil des Netzwerk-Gesamtbetriebs aufgebaut werden. Allerdings unterscheiden sich die technischen Details, so dass hier ein neuer Betriebsbereich mit neuen Produkten erforderlich wird. Dabei ist davon auszugehen, dass ein entsprechend geeigneter WLAN-Betrieb folgende Leistungsmerkmale haben muss:

- Abdeckung aller WLAN-Standards
- Zentrale Konfiguration aller Access Points
- Zentrales Monitoring der Betriebssituation aller Access Points
- Regelbasierte Verarbeitung der Meldungen der Access Points mit Korrelation zur Reduzierung der Meldemenge, insbesondere für die WLAN-typischen Qualitätswerte
- Permanente Überwachung der Kapazitätssituation
- Unterstützung einer Veränderung der Kanalzuweisung zu den Access Points und deren Sendestärke, um die Kapazität zu erhöhen
- Ausfallerkennung und Unterstützung von Redundanz-Maßnahmen
- Reporting mit Trendanalyse, aufgeteilt nach Zellen, Bandbreitennutzung pro Applikation, pro Teilnehmer, bei Einsatz von QoS pro Qualitätsstufe/Priorität/VLAN
- Gezielte Ermittlung von Zugangszeit/Delay/Laufzeit/Packet-Loss

Es ist zu überprüfen, ob mit künstlichen Teilnehmern Service-Level-Überprüfungen durchgeführt werden sollen.

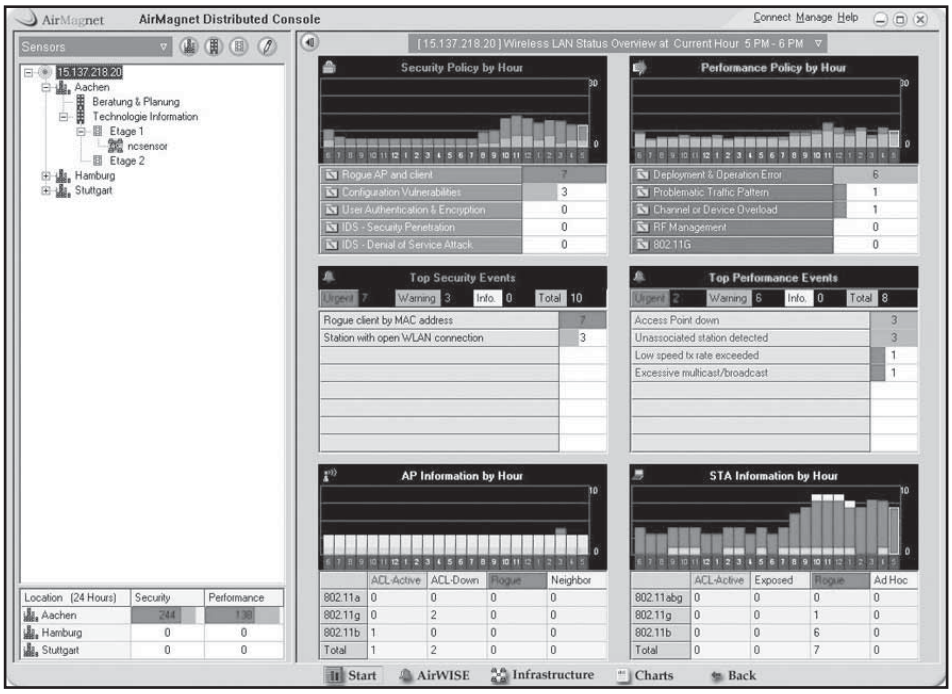


Abbildung 7: Überwachungstool AirMagnet

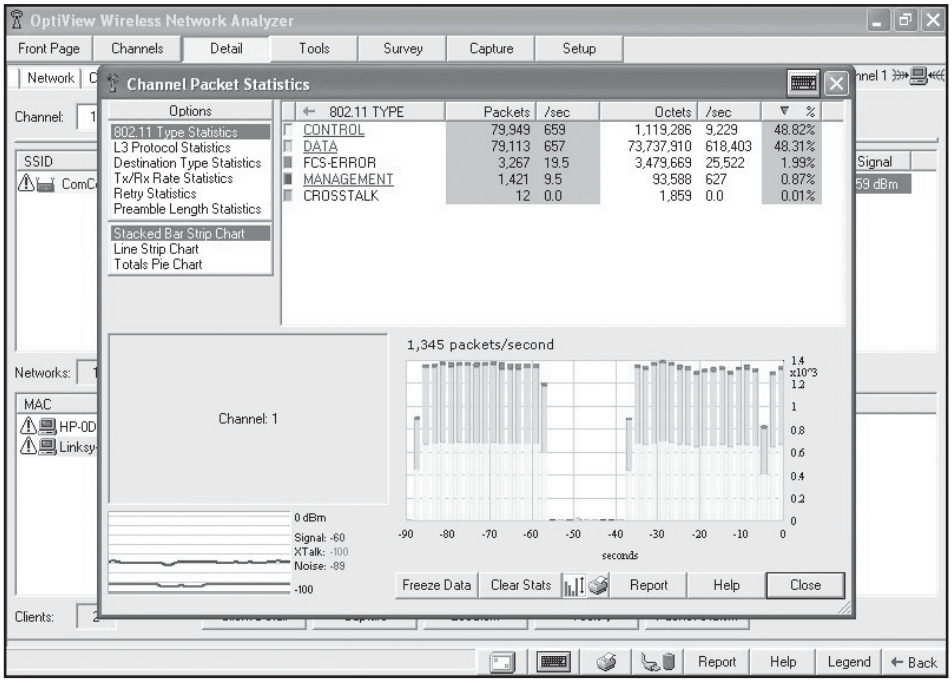


Abbildung 8: Trouble-Shooting-Tool optiView von Fluke

10. Neubausituation

WLAN-Installationen sind bereits heute preiswerter als Kabelgebundene Installationen. Noch hinkt der Vergleich, leisten doch Gigabit-LANs die höhere Bandbreite. Doch dies ist eine reine Zeitfrage. Innerhalb der nächsten 5 Jahre wird es kaum noch ein Kontra-Argument gegen WLAN-Technik geben, die Installationen werden aber mindestens 40% günstiger sein als bei Kabel-Netzwerken. Nicht aus Zufall behindern wichtige Hersteller die WLAN-Entwicklung.

Voraussichtlich wird sich auf absehbare Zeit die Planung so genannter Overlay-Netzwerke durchsetzen. Bei Overlay-Netzwerken werden Wireless-Netzwerke mit Kabelgebundenen Netzwerken gezielt

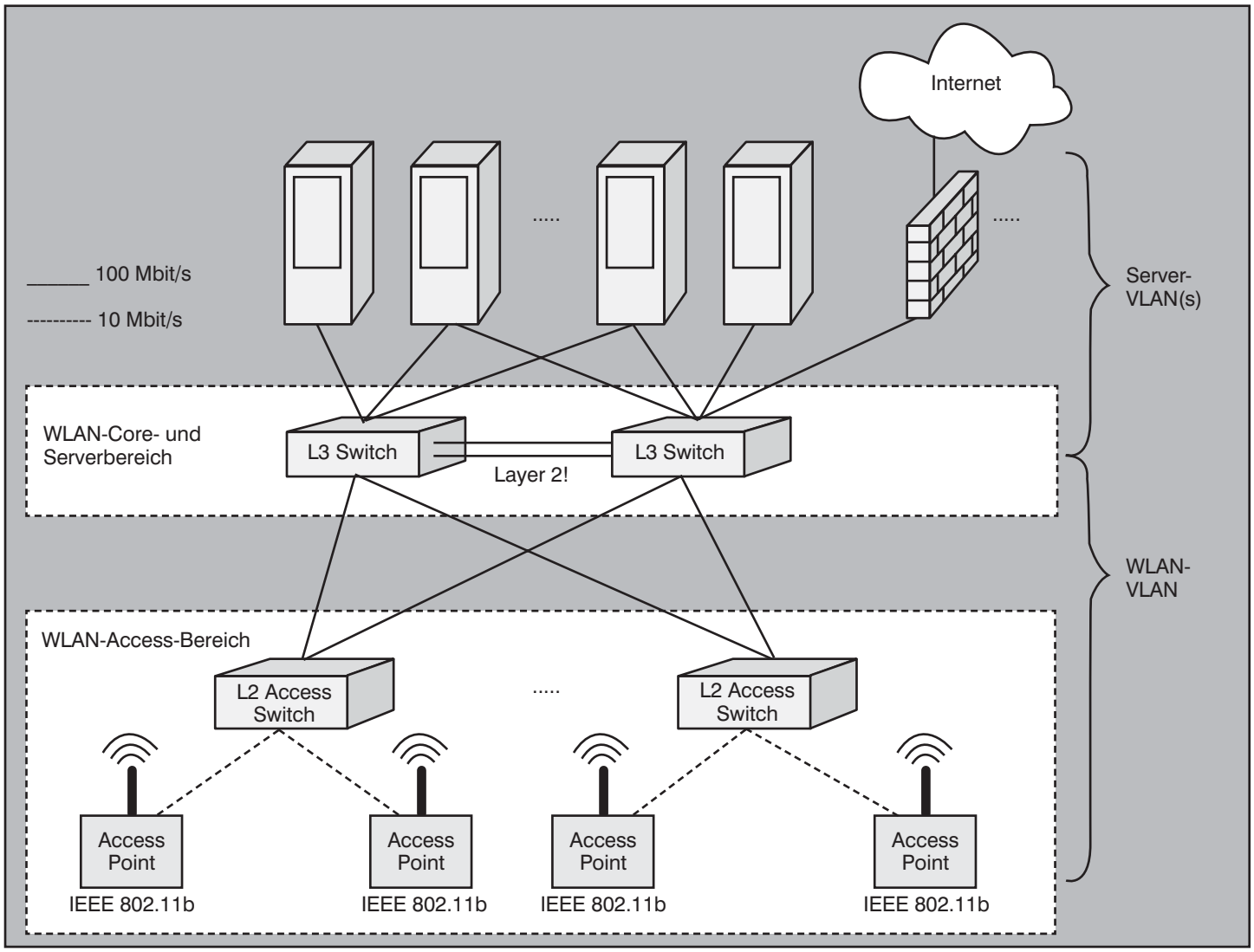


Abbildung 9: WLAN-Absicherung mit VLANs

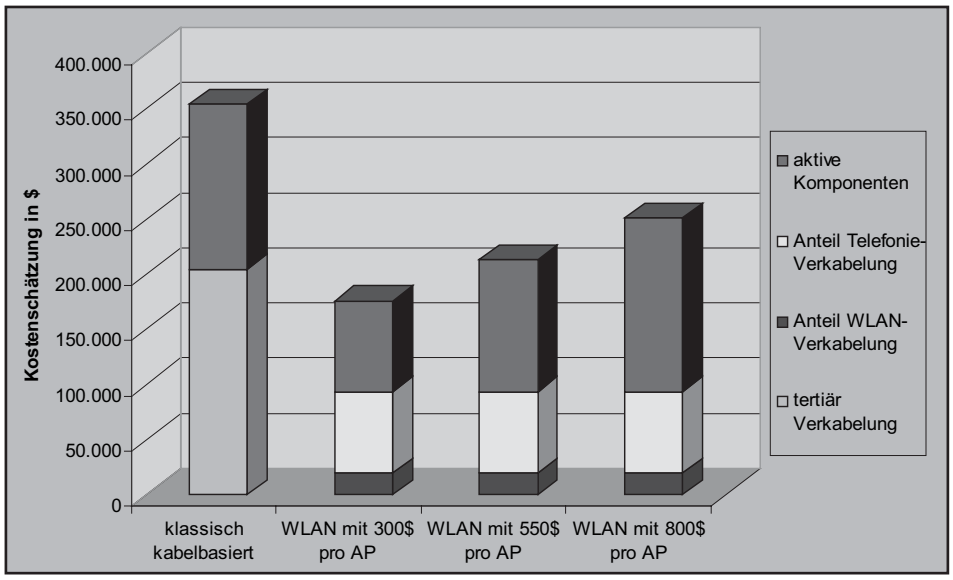


Abbildung 10: Kostenvergleich kabelbasiertes Netzwerk vs. Wireless LAN

gemischt. Die ist erstaunlich wirtschaftlich, da zum Beispiel durch ein WLAN die in der Regel im Kabel vorgesehenen Überkapazitäten abgebaut oder ganz vermieden werden können. Statt wie sonst üblich pro Teilnehmer 2 Anschlüsse zu planen, wird in der einfachsten Stufe 1 Anschluss geplant. Damit entstehen die so genannten Overlay-Stufen, die sich grundsätzlich nur auf die Tertiärverkabelung beziehen. Diese sind wie folgt definiert:

- Overlay 0: Komplettversorgung durch Kabel, Wireless als Ergänzung, Vollversorgung kann aber durch Kabel erfolgen

- Overlay 1: Pro Teilnehmer ein Kabelanschluss, aber keine weiteren Reserven. Da hierbei ein Teilnehmer mit einer definierten Fläche gleichgesetzt wird (zum Beispiel 10 qm), kann dies bei höheren Teilnehmerdichten zur Unterversorgung

führen. Diese sowie der Anschluss der kompletten Peripherie werden auf der Basis von Wireless ausgeglichen.

- Overlay 2: Komplette Versorgung der normalen Teilnehmer durch Wireless. Server und Power-User werden durch Kabel versorgt. Kritisch im Bereich von Power-Usern, da diese bei Umzügen ihren Standort wechseln

- Overlay 3: Nur noch Server werden im Tertiärbereich durch Kabel versorgt. Overlay-Stufe 3 wird für viele Anwendungen Gigabit-Wireless voraussetzen, also erst in einigen Jahren zum Einsatz kommen. Wie kann man sich heute darauf vorbereiten? Wie kann in einer aktuellen Neubausituation der wirtschaftlich und technisch aktuelle Mix aus Funk und Kabel gefunden werden?

Auf Dauer wird die Planung von Overlay-Netzwerken für Neubauten zum Standard werden. Die wirtschaftlichen Vorteile sind so groß, dass nach der Überwindung der zum Teil noch gegebenen emotionalen Ablehnung von Wireless-Netzwerken der Weg in diesen Netzwerktyp gehen wird.

11. Spezielle Anwendungsbereiche

Es gibt eine Reihe von Anwendungsbereichen, die quasi nur auf WLANs gewartet haben. Von der Ablösung des betagten und teuren Bündelfunks über den Bergbau bis hin zu Transport- und Warenlogistik reicht das Spektrum. Auch der gesamte Gesundheitsbereich benötigt dringend Wireless-Installationen, um seine Abläufe weiter optimieren zu können. Ein Teil des heutigen Wireless-Marktes lebt von diesen Spezialanwendungen. Da hier häufig keine wirklich bessere Alternative besteht, werden Wireless-Netzwerke hier schnell umgesetzt.

Gerade in diesen Bereichen sollte auf die Zukunftsfähigkeit der Lösung geachtet werden. Ein hoher Projektdruck, eine beschränkte Produktauswahl von Spezialprodukten, eine geringe Zahl von Anbietern sind ideale Voraussetzungen für Fehlentscheidungen. Auch Speziallösungen sollten mit einem Design erfolgen, das für mindestens 3 Jahre tragfähig ist.

12. Hot-Spot-Anwendungen

Der Betrieb von WLAN-Hot-Spots ist in vielen Anwendungsbereichen sinnvoll, sei es für unternehmensinterne Nutzung oder für öffentliche Nutzung. Gerade aber mit dem Aufbau von Hot-Spots sind viele Fragen verbunden, die deutlich über die normale Wireless-Installation hinausgehen. Wie erfolgt die Anmeldung eines Teilnehmers? Wie können Kostenerfassung, Abrechnung und Inkasso umgesetzt werden? Welche Sicherheitsanforderungen sind seitens der Teilnehmer zu berücksichtigen? Was bringt der neue Standard, der die sichere Einwahl in einen Hot-Spot regeln soll? Sind Traffic-Shaping oder Bandbreitensteuerung erforderlich? Müssen bestimmte Anwendungen wie Voice gezielt unterstützt werden, muss also ein Hot-Spot QoS umsetzen?

Wie an dieser Diskussion zu erkennen, werden Wireless-LANs durch die Vielzahl der Potenziale, die sie bieten, eine zunehmend große Rolle im Design von Netzwerken spielen. Aber gerade der Aspekt der Zukunftssicherheit der Investitionen und die enormen noch zu erwartenden Entwicklungen erfordern ein darauf abgestimmtes Konzept. Eine sichere und zukunftsorientierte Planung ist heute möglich, wenn die zuvor beschriebenen Rahmenbedingungen eingehalten werden. An vielen der dargestellten Diskussionspunkte ist erkennbar, dass aus heutiger Sicht die Zukunft für professionelle WLANs im Bereich der 5 GHz-Netzwerke liegt. Da auf jeden Fall eine rückwärtskompatible Lösung erforderlich ist, muss in jedem Fall mit einem Parallelbetrieb von 2,4 GHz und 5 GHz gerechnet werden.

Wir werden diese Aspekte auf unserem Wireless-LAN-Forum 2004 im November besprechen. Dort veröffentlichen wir auch unsere neuesten Messergebnisse exklusiv, sprich sie können diese Ergebnisse nur als Teilnehmer dieses Forums erhalten. Parallel wird es eine Reihe interessanter Projektberichte geben. Wie immer werden wir die Situation des Marktes, die Leistungsfähigkeit der angebotenen Produkte und die zukünftige Entwicklung analysieren und mit Ihnen diskutieren.

Literatur

1. Wireless kontra Kabel
   Autoren: Mark Groten, Dr. Simon Hoff
   Herausgeber: ComConsult Research

2. Wireless LAN Evaluierung
   Autor: Dipl.-Math. Cornelius Höchel-Winter
   Herausgeber: ComConsult Research

3. Wireless LAN Antennenguide
   Autoren: Dipl.-Math. Cornelius Höchel-Winter, Dr. Simon Hoff, Dr.-Ing. Joachim Wetzlar
   Herausgeber: ComConsult Research

CCNE

ComConsult Certified Network Engineer

Lokale Netze
27.09. - 01.10.04 in Aachen
06.12. - 10.12.04 in Aachen
21.02. - 25.02.05 in Aachen
25.04. - 29.04.05 in Aachen
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
27.09. - 01.10.04 in Berlin
06.12. - 10.12.04 in Bonn
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
21.11. - 25.11.05 in Bonn

Internetworking
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen
28.02. - 04.03.05 in Aachen
30.05. - 03.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Ethernet Technologien - neuester Stand
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen
14.03. - 18.03.05 in Aachen
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
08.11. - 12.11.04 in Aachen
21.02. - 25.02.05 in Aachen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
27.09. - 01.10.04 in Aachen
14.02. - 18.02.05 in Aachen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
22.11. - 26.11.04 in Aachen
11.04. - 15.04.05 in Aachen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare mit Etherreal in Kombination mit Fluke Net-tool € 7.500.-- zzgl. MwSt. (Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
11.10. - 15.10.04 in Bonn
14.02. - 18.02.05 in Bonn
25.04. - 29.04.05 in Bonn
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
13.09. - 15.09.04 in Köln
15.11. - 17.11.04 in Köln
28.02. - 02.03.05 in Bonn
30.05. - 01.06.05 in Köln
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
04.10. - 08.10.04 in Aachen
06.12. - 10.12.04 in Aachen
18.04. - 22.04.05 in Aachen
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

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

Impressum

Verlag:
Dr. Suppan International institute b.v
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen