ComConsult Research

Der Netzwerk Insider

März 2005

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

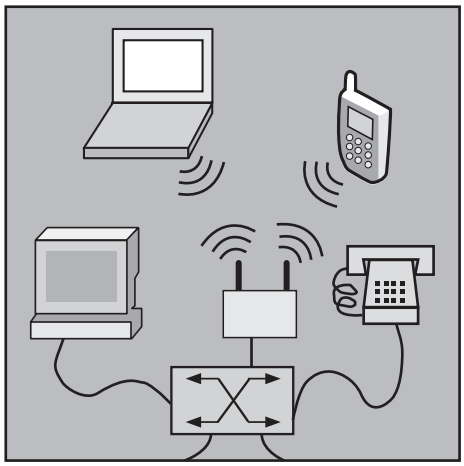
von Dipl.-Inform. Petra Borowka - Teil 2

3. Wireless Lösungen

3.2 Wireless LAN (WLAN)

Redundanz

Aufgrund der Mobilität der Benutzer einerseits und Störverhalten von nah nebeneinander positionierten Access Points andererseits ist das Thema Redundanz nicht wie bei wireline Technologien durch einfache physikalische Dopplung, Mehrfachanbindungen und standardisierte Layer-2/Layer-3 Redundanzverfahren abzuhandeln. Die physikalische Dopplung mit defaultmäßigem Betrieb wäre im Gegenteil erst einmal kontraproduktiv aufgrund überschneidender Antennen-



bereiche und des damit erzeugten Leistungseinbruchs. Die Betrachtung von Redundanzlösungen für Wireless LAN hängt daher immer auch mit den Aspekten Sendeleistung, effiziente Ausnutzung der verfügbaren shared LAN Kapazität und fehlertolerantes Roaming zusammen.

weiter auf Seite 22

Zweitthema

Herausforderungen der RZ-Konsolidierung: Datacenter im Internet

von Dr. Behrooz Moayeri

Die Konzentration von Rechenzentren auf einen oder wenige Standorte ist einer der wichtigsten IT-Konsolidierungstrends unserer Zeit. Viele Unternehmen fassen die von ihnen benötigten IT-Ressourcen in immer wenigeren Data Centern zusammen und lassen die Benutzer an anderen Lokationen über ein Wide Area Network (WAN) auf diese Data Center zugreifen. Global oder international agierende Unternehmen konsolidieren ihre RZ, indem sie in drei oder vier Regionen die Systeme aufstellen, auf die zur Abwicklung der Applikationen zugegriffen werden muss. Dass es sich dabei immer noch um mehr als einen Standort für die Data Center handelt, hängt damit zusammen, dass erstens die Verteilung geschäftskritischen Equipments auf geografisch entfernte Orte das Überleben auch größerer Katastrophen sichert, zweitens Netzverbindungen zwischen verschiedenen Welt-Regionen wie zwischen Europa und Fernost immer noch recht kostspielig sind und drittens global tätige Firmen ohnehin dafür sorgen müssen, dass nach dem „follow-the-sun“-Prinzip Personal für die technische Unterstützung von IT-Prozessen rund um die Uhr verfügbar ist, was mit einer Verteilung der IT-Mitarbeiter auf die drei Regionen Europa, Nordamerika und Fernost erreicht wird.

Seite 6

Top-Event

ComConsult IT-Sicherheits-Forum 2005

auf Seite 15

Zum Geleit

Wireless LANs: wohin geht der Weg?

auf Seite 2

Report des Monats

Sicherheit in Wireless LANs mit 802.11i und WPA2

auf Seite 19

Zum Geleit

Wireless LANs: wohin geht der Weg?

Wie in jedem Jahr, so werden wir auch in diesem Jahr exklusiv über die Ergebnisse einer Reihe von ComConsult Research Studien sprechen. Eine dieser Studien befasst sich mit der Zukunft und Investitionssicherheit im Bereich Wireless LAN. Dabei ist gerade der Bereich der Investitionssicherheit mit einer hohen Aufmerksamkeit zu versehen. Im Folgenden nur einige Auszüge aus den aktuellen Arbeiten. Mehr dazu exklusiv auf dem Netzwerk-Redesign Forum vom 18.-21. April 2005 in Königswinter.

Seit einigen Wochen überschlagen sich die Hersteller von Wireless LANs wieder mit Produktankündigungen. Der Markt ist in extremer Bewegung. Gegebener Anlass für die Hektik war die CES Elektronic Consumer Show in Las Vegas (mit einer sehr hohen Bedeutung für den amerikanischen Markt) und ist die bevorstehende CeBIT. Diese beiden Veranstaltungen stecken gleichzeitig die typischen Eckpunkte der aktuellen Wireless-Entwicklung ab. Und diese Eckpunkte drifften immer mehr auseinander, so dass eine immer stärkere Zweiteilung des Wireless-Marktes zu beobachten ist.

Auf der einen Seite steht der riesige Hifi- und Elektronik Konsumer-Markt, bei dem Wireless in den Mittelpunkt der Anlagentechnik gerückt ist. Ziel ist es, die verschiedenen Anlagenkomponenten einer Hifi- und TV-Lösung über ein Wireless-LAN herstellerneutral zu verbinden. Entsprechend umfangreich ist das Angebot derartiger Lösungen auf der CES gewesen. Der Trend geht dabei immer mehr weg vom PC im Wohnzimmer hin zum Media-Server, der zentral ein Wohngebäude versorgt. Auf dem Media-Server sind Foto, Video und Musik gespeichert und können über spezielle Clienten im WLAN in die entsprechenden Hifi-Anlagen oder Fernseher eingespeist werden. Musik- und Videorekorder dienen als Einspeisegerät für den zentralen Media-Server. Von der Gerätetechnik her gibt es verschiedene Ansätze zur Realisierung der Media-Server. Die IT-Anbieter wie Microsoft sehen hier einen typischen Einsatzbereich für spezielle Media-PCs. Die traditionellen Hifi-Anbieter sehen hier eher weiterentwickelte Videorekorder mit sehr großen Plattensystemen (siehe Panasonic, wobei diese Geräte häufig verkappte Linux-Systeme sind).

Nun ist aber unschwer festzustellen, dass heute Wireless-LAN nicht wirklich für die Herausforderungen des Konsumer-Marktes gerüstet ist. Es erfüllt die gegebenen Anforderungen auch nicht annähernd.

Kernanforderungen des Konsumer-Marktes sind:

- Ausreichende Kapazität für die parallele Übertragung von HDTV, 2 weitere MPEG2-Datenströme und 3 MP3-Datenströme. Zusammen erfordert das eine Übertragungsrate von 40 bis 50 Mbit/s Nutzdaten. Rechnet man das unter Berücksichtigung des aktuellen WLAN-Medienzugangsverfahrens in eine Rohdatenrate um, dann besteht ein Kapazitätsbedarf von ca. 100 Mbit/sek.
- Abdeckung eines ganzen Gebäudes mit einem zentralen Access-Point. Diese Anforderung ist kritisch, da sich zum Beispiel die amerikanische Gebäudetechnik sehr von der deutschen unterscheidet, die Orientierung aber am amerikanischen Markt erfolgt. Konkret sollte ein Access-Point einen Radius von 20m inkl. 3 Wände mit einer Nutzdatenrate von 50 Mbit/sek. versorgen können
- Stabile Übertragung ohne Einbrüche, diese würden eine Videoübertragung massiv stören

Vergleicht man diese Anforderungen mit dem Leistungsspektrum aktueller genormter Produkte, dann ist festzustellen, dass weder die Kapazität noch die Stabilität gegeben ist. Die heutigen WLAN-Standards sind im Einsatzgebiet der Konsumer-Elektronik ungeeignet. Auch wenn die Bandbreite für MP3 sicher ausreicht, die Stabilität sicher nicht.

Hinzu kommt ein Faktor, der eine immer größere Dimension annimmt. Dies ist der Störeinfluss anderer Anwendungen im 2,4 GHz Band. Hier nimmt gerade im Konsumer-Markt das Angebot entsprechender Produkte lawinenartig zu.

Da speziell dieser Markt aber riesig ist und hohe Umsätze und Gewinne locken, preschen immer mehr Anbieter mit nichtstandardisierten Lösungen auf den Markt. Nachdem dies lange Zeit scheinbare Fortentwicklungen bestehender Standards waren, wie die 11g+ Lösung, so beziehen sich immer mehr Anbieter auf den zukünftigen 11n-Standard. Dies ist mehr als problematisch, da gerade dieser Standard von zwei gegensätzlichen Hersteller-Lagern blockiert wird. Auf der einen Seite die Gruppe der Hersteller, die am Konsumer-Markt orientiert sind und die vor allem eine schnelle Lösung mit sofortiger Produktverfügbarkeit wollen. Auf der anderen Seite die Gruppe der Hersteller, die es endlich richtig machen wollen, nachdem die bisherigen Standards mehr Funktechnik für Arme waren. In der Normung ist damit eine Blockade eingetreten, die jede Vorhersage über die zeitliche Entwicklung schwierig macht. Im Endeffekt hat die Schnellschussgruppe alle strategischen Vorteile auf ihrer Seite, da sie in der Lage ist bereits jetzt Vorserienprodukte auf den Markt zu bringen. Je länger die Blockade dauert desto höher wird der Druck auf die andere Gruppe. Es ist also zu befürchten, dass der 11n-Standard weit von seinen ursprünglichen Zielen entfernt bleiben wird.

Die im Moment als Vorserienprodukte auf den Markt geworfenen Produkte arbeiten nach dem MIMO-Prinzip, nach dem die Übertragung in mehrere parallele Übertragungen aufgeteilt wird, die über parallele Sender- und Empfängerantennen abgestrahlt werden.

Auf dem Markt werden diese Produkte von Belkin und Linksys angeboten (Linksys hat das Produkt gerade erst auf den Markt gebracht, Belkin vertreibt es seit Mitte 2004, beide basieren auf einem identischen Chip). Da zu befürchten ist, dass sich dieses „Schnell-Aber-Schmutzig-Lager“ durchsetzt, haben wir das Belkin-Produkt im Labor vermessen. Eine Motivation dazu war auch, dass dies zuvor von anderen Labors bereits gemacht wurde, die zu sehr guten Ergebnissen gekommen waren. Uns hat vor allem die Grundfrage interessiert, welche Potenziale in einer MIMO-Technologie liegen.

Wireless LANs: wohin geht der Weg?

Die Ergebnisse in kurzen Worten
(Details auf dem Forum):

- Im Idealzustand erreicht das Belkin-Mimo-PreN-Produkt herausragende Werte mit Reichweiten von deutlich über 20m und einer Rohdatenrate von 108 MBit/s auch durch 3 bis 4 Wände hindurch
- Bereits in diesem Idealzustand konnten wir keine höheren Datenraten als 30 Mbit/s feststellen, so dass eine sehr hohe Verlustleistung festzustellen ist
- Das Produkt arbeitete in unseren Tests in keiner Weise stabil, an einzelnen Standorten konnte reproduzierbar überhaupt keine sinnvolle Leistung erzielt werden
- Auch an Orten, an denen das Produkt bei einer Messung gut arbeitete, konnte im operativen Langzeitbetrieb über mehrere Tage immer wieder ein massives Einbrechen der Leistung beobachtet werden. Da wir uns trotz mehrfacher Messungen und sehr professioneller Tools unsicher waren, haben wir die Messungen mit unterschiedlichen Belkin-Produkten sowohl in Neuseeland als auch in Aachen durchgeführt. Die Ergebnisse decken sich, wobei in Neuseeland eine Rohdatenrate von 40 Mbit/s erreicht wurde. Wir konnten nachweisen, dass das Produkt massiv sensibel auf andere Anwendungen im 2,4 GHz-Bereich reagiert. Die Laborumgebungen in Neuseeland sind funktechnisch sehr sauber, in Aachen existieren starke Einflüsse anderer WLAN-Netzwerke

Unser Ergebnis:

- Wie immer auch die 11n-Lösung aussehen wird, ihr Potenzial ist riesig. Sie wird die heutige Situation deutlich verbessern und den Bedarf der Konsumertechnik erfüllen
- Auch wenn die am Konsumer-Markt orientierten Hersteller auf das 2,4 GHz-Band fixiert sind, da sie die Rückwärtskompatibilität mit dem 11b-Standard suchen, muss immer mehr festgestellt werden, dass die Interferenzen zwischen verschiedenen Anwendungen im 2,4 GHz-Band zu schnell zunehmen, dass es für professionelle Anwendungen schon bald nicht mehr tragfähig sein wird. Hier kann die Zukunft von Enterprise-WLANs auf keinen Fall liegen
- Mindestens das heutige Belkin-Produkt hat in unseren Labortests nicht überzeugt, dabei weichen unsere Ergebnisse deutlich von den Ergebnissen anderer Labors ab. Allerdings haben diese nach unserem Verständnis weder Langzeit-Stabilitätstests gefahren noch die Sensibilität gegenüber anderen 2,4 GHz-Sendern berücksichtigt

So viel zum Konsumer-Markt. Dem steht diametral der Enterprise-Markt gegenüber. Dieser wird immer stärker vom Bewusstsein geprägt, dass wir eine flächendeckende Wireless-LAN-Infrastruktur brauchen und dass diese wirtschaftlich ist. Vor allem der Anwendungsbereich Voice over WLAN zeigt so erhebliche wirtschaftliche Vorteile, dass die Tendenz hier klar ist.

Aus diesem Anspruch der Flächendeckung und der auch hier zu beobachtenden immer weiter zunehmenden Störung anderer 2,4 GHz-Sender können folgende Anforderungen an einen zukünftigen Enterprise-WLAN-Standard abgeleitet werden:

- Stabilität, Stabilität, Stabilität. Voice und Video werden zukünftige Kernanwendungen sein, auch der Markt für Kollaborationsprodukte auf Basis von IP-Telefonie expandiert sehr stark. Er wird bereits jetzt in den USA als der eigentliche Anwendungsbereich für IP-Telefonie auf Basis von SIP gesehen. Diese Art von Anwendung kann stark schwankende Übertragungsleistungen nicht verkraften
- Wechsel in den 5 GHz-Bereich, um sowohl den zunehmenden Störungen des 2,4 Ghz-Bereichs auszuweichen als auch eine höhere Kanalzahl zu haben
- Hohe Zahl an überschneidungsfreien Kanälen. Bedingt durch DFS muss diese Zahl höher sein als intuitiv angenommen. WLANs im 5 GHz Bereich müssen anderen Anwendungen in diesem Bereich, speziell Radar, durch Wechsel des Frequenzbandes ausweichen. Will man nun auch ausreichend Reserve beim Wechsel haben, braucht man eine höhere Zahl von Bändern
- Zuweisung von Verkehrsklassen an Kanäle, weg von der Prioritäts-gesteuerten QoS-Lösung. Das hört sich dramatischer an als es klingt, man wird mit 2 oder 3 Verkehrsklassen auskommen
- Nutzdatenrate von mehr als 100 Mbit/s, mehr Leistung als bei 100 Mbit/s Ethernet

Es ist klar zu erkennen, dass diese Anforderungen weit über die Anforderungen des Konsumer-Marktes hinaus gehen. So haben sich im Enterprise-Markt in den letzten Monaten auch völlig andere Architekturen entwickelt. Seit dem Einstieg von CISCO in den Controller-gesteuerten WLAN-Markt ist diese Technik, die zuvor nur von Startups angeboten wurde, im Markt zum Standard aufgerückt. Enterprise-WLANs bestehen aus Access Points, die von zentralen Controllern gesteuert werden.

Gegenstand der Steuerung sind:

- Zugewiesene Kanäle pro Access Point
- Sendeleistungen
- Redundanzschaltungen, Reaktion auf ausgefallene Access Points und Controller
- Erkennung unerlaubter Access Points
- Layer-3-Roaming

Der Ursprung der Controller-gesteuerten WLANs liegt im Bereich Roaming. Durch den Controller wird der Zellwechsel stark vereinfacht. Der Bedarf für eine dedizierte Kanal- und Leistungssteuerung setzt sich im Markt aber immer weiter durch. Bisher wurde diese Anforderung, die durch ComConsult Research seit über einem Jahr als existenziell gekennzeichnet wurde, im Allgemeinen nicht sehr ernst genommen. Seitdem CISCO den genau hierauf spezialisierten Hersteller Airespace gekauft hat, ist klar, wohin der Markt geht.

Kernempfehlungen von ComConsult Research für Enterprise-WLANs werden wir im Detail auf dem Netzwerk-Redesign Forum geben.

Wer wird sich in der 11n-Standardisierung durchsetzen, der Konsumer-Markt oder der Enterprise-Markt? Voraussichtlich der Konsumer-Markt. Entscheidend aus Sicht der gegebenen Anforderungen auf der Enterprise-Ebene werden sein

- Orientierung am 5 GHz-Band
- Stabilität
- Mehr als 100 Mbit/s Nutzdatenrate

Meine Prognose: da Stabilität die Kernanforderung für den Konsumer-Markt ist, wird dies kommen. Im Bereich 5 GHz sind die bisherigen Standard-Entwürfe an diesem Bereich orientiert. Auch der von Belkin und Linksys eingesetzte Vorserienchip unterstützt von Hause aus auch das 5 GHz-Band mit 3 Antennen. Dies lässt hoffen. Bei der Nutzdatenrate habe ich im Moment keine Hoffnungen. Stabile und höhere Nutzdatenraten würden erhebliche Änderungen am Medienzugangsverfahren und an der Funktechnik erfordern. Im Moment sieht es dafür nicht gut aus, auch wenn die notwendigen Änderungen konkret bekannt sind (siehe dazu im Detail diverse Vorträge und Artikel von ComConsult Research und Dr. Kauffels).

Aber egal wie die Entwicklung verläuft, im Jahr 2006 werden wir den nächsten Leistungssprung in der Wireless-LAN-Technik haben. Auch wenn es aus heutiger Sicht ein eher kurzer Sprung werden wird.

Trotzdem sind die zu erwartenden Unterschiede im Vergleich zu den heute verkauften und eingesetzten Produkten massiv. Wer hier nicht in die völlig falsche Richtung investieren will, der sollte sich auf die kommenden Änderungen einstellen.

Ich freue mich auf eine spannende Diskussion auf dem Netzwerk-Redesign Forum.

Ihr
Dr. Jürgen Suppan

Top-Event

Netzwerk-Redesign Forum 2005 Fast ausgebucht - sichern Sie sich die letzten Plätze

Vom 18. - 21. April 2005 veranstaltet die ComConsult Akademie den Kongress „Netzwerk-Redesign Forum 2005“ in Königswinter. Der Kongress analysiert die aktuellsten Entwicklungen der Netzwerk-Technologie und bewertet Marktrends und Produktentwicklungen.

Wie entwickeln sich Netzwerke weiter? Wie sehen geeignete Strategien und Konzepte aus? Was passiert im Markt? Wo liegen Tücken und Fallstricke in aktuellen Technologien?

Die passenden Antworten liefert das Netzwerk Redesign Forum 2005, das seit 10 Jahren zu den Top-Events der Branche zählt.

Mit einer Mischung aus hochaktuellen Technologie-Vorträgen, den exklusiven Ergebnissen neuester Technologie-Untersuchungen sowie diversen Projekterfahrungen und vielen begleitenden Diskussionen und Gesprächen ist diese Veranstaltung ein Muss für jeden, der beruflich mit Netzwerken zu tun hat.

Im Mittelpunkt des Netzwerk-Redesign-Forums 2005 steht die Frage, wie das Design bestehender Netzwerke zur Erfüllung der immer weiter gehenden Kommunikations-Anforderungen verbessert werden kann.

Das Redesign-Forum 2005 bietet folgende hochaktuelle Themenblöcke:

- Top-Analyse unseres Labors: neue Kommunikations-Anforderungen an Netzwerke
- Netzwerk-Redesign
- Standardisierung und Technologie-Entwicklung
- Optimierung des Netzwerk-Betriebs
- Hersteller und Produkte
- Sicherheit und Netzwerke
- WAN/Corporate Networks im Umbruch
- IP-Telefonie erfolgreich einsetzen
- Wireless LANs

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die Intensiv-Trainings für den 4. Tag entnehmen Sie bitte der Programmübersicht auf den folgenden Seiten.

Sie sehen, das Netzwerk Redesign Forum 2005 wird seinem Ruf als die führende deutsche Kongressveranstaltung zu Netzwerk-Technologien wieder voll gerecht. Mittlerweile im 10. Jahr wird sich hier auch 2005 die Branche treffen.

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

Zögern Sie nicht und sichern Sie sich einen Platz auf unserer Top-Veranstaltung des Jahres 2005.

Auf dem Forum werden Sie von unserem Spitzen-Moderatoren begrüßt:

Dr. Jürgen Suppan,
Dr. Franz-Joachim Kauffels

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzwerk-Redesign Forum 2005

Ich buche den Kongress
Netzwerk-Redesign Forum 2005
vom 18.04. - 21.04.05 in Königswinter

☐ **mit Workshop € 1.990,- zzgl. MwSt.**
☐ **ohne WorksHop € 1.690,- zzgl. MwSt.**

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

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

Sonderaktion

Sonderaktion ComConsult Zertifizierungen

mit ipod Shuffle und allen Insider-Jahrbüchern bis zum 31.03.05

Die Zertifizierungen von ComConsult sind jetzt sieben Jahre alt. Mehrere Tausend Teilnehmer haben in dieser Zeit die Kurse besucht. Das hohe Niveau der Ausbildung und die Herstellerneutralität haben zu der breiten Akzeptanz im Markt geführt. Die Inhalte der Ausbildungen werden laufend aktualisiert und dem neuesten technischen Stand angepasst. Auch nach Abschluss der Zertifizierungen werden die Teilnehmer durch unseren Netzwerk-Insider und spezielle Update-Veranstaltungen auf dem neuesten Stand gehalten.

Wir sind der Ansicht, dass dies ein Anlass zum Feiern ist. Aus diesem Grund erhalten alle Teilnehmer, die sich bis zum 31.03.05 zu einer Zertifizierung anmelden, unsere neue **„Apple ipod Shuffle Netzwerk-Insider-Special-Edition“** kostenlos als Teil ihres Ausbildungspakets mit allen Insider Jahrbüchern inklusive 2004 und den ComConsult Research-Studien „Wireless kontra Kabel: ein Kostenvergleich“, „Wireless LAN Antennenguide“ und „LAN-Verkabelung neuester Stand“.

ComConsult Certified Network Engineer

Fundiertes Wissen über Netzwerke ist heute für viele Bereiche der Schlüssel zum Erfolg. Die Ausnutzung der vielfälltigen Möglichkeiten und Mechanismen Lokaler Netzwerke erfordert dabei ein erhebliches und tiefgehendes Hintergrundwissen.

Spätestens beim Auftreten von Störungen ist dieses Wissen gefragt. Dabei ist elementares Netzwerk-Wissen nicht auf Planung und Betrieb von Netzwerken reduzierbar, auch die Betreiber und Betreuer von PCs und Servern benötigen fundiertes Wissen für den sicheren Umgang mit Netzwerken und die saubere Abgrenzung von System- und Netzwerk-Fragen.

Mit dem ComConsult Certified Network Engineer hat die ComConsult Akademie die anerkannte herstellerneutrale Ausbildung zum Netzwerkprofi geschaffen.

ComConsult Certified Trouble Shooter

Störungen in Lokalen Netzwerken werden immer komplexer. Die Ursache einer Störung kann im Bereich der Anwendung, des Betriebssystems, des IP-Protokolls oder des reinen L2/L3-Netzwerks bis hin zum Kabel oder zur Funkübertragung liegen. Die schnelle und kompetente Analyse und Beseitigung der Störung erfordert nicht nur die geeigneten Werkzeuge sondern vor allem methodisches Arbeiten und das darauf optimierte Querschnittswissen über alle beteiligten Technologien. Wir vermitteln Methode und Wissen mit der Ausbildung zum ComConsult Certified Trouble Shooter. Sie liefert auf der einen Seite das Wissensfundament für die professionelle Beherrschung von Netzwerken und trainiert auf der anderen Seite die systematische und nachhaltige Beseitigung von Störungen.

ComConsult Certified Security Expert

Mit dem ComConsult Certified Security Expert (CCSE) bietet die ComConsult Akademie eine systematische Ausbildung zum/zur Sicherheits-Spezialisten/in für Netzwerk- und IT-Technologien an. Die Ausbildung ist so aufgebaut, dass alle wesentlichen Technologien vom Netzwerk bis zur Clienten-Sicherheit im Sinne des stufenweisen Aufbaus einer Gesamtlösung abgedeckt werden.

Die Ausbildung zum CCSE berücksichtigt anerkannte Sicherheits-Standards. Sowohl das Grundschutzhandbuch des BSI als auch die international angesehene BS7799 fließen in die Ausbildung ein. Damit wird gleichzeitig das Wissen vermittelt, auf dessen Basis Unternehmen sich für eine zukünftige Sicherheits-Zertifizierung vorbereiten können.

Zweitthema

Herausforderungen der RZ-Konsolidierung

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH, Aachen. Er hat in den letzten 15 Jahren zahlreiche Unternehmen und Organisationen bei der Konzipierung von IT-Infrastruktur-Konzepten, u. a. beim Aufbau standortübergreifender Netze, beraten.

Die RZ-Konsolidierung birgt jedoch Herausforderungen in sich. Nach dem Motto „it's all on the Web" soll das Unternehmensnetz alle Ressourcen zu jeder Tageszeit und an jedem Kalendertag zur Verfügung stellen. Das Netz muss performant genug sein, um die Antwortzeit bei IT-Anwendungen nicht ins Unerträgliche steigen zu lassen. Es muss zu 99 + x % verfügbar sein (denn selbst 1 % Ausfallzeit entspricht fast 90 Stunden im Jahr). Angreifer oder schadensstiftende Software wie Viren und Würmer dürfen dieses weltumspannende WAN möglichst weder lahm legen noch unter ihre Kontrolle bringen und die Vertraulichkeit der übertragenen Informationen gefährden können. Und das alles zu einem Preis, den die Unternehmen für die RZ-Konsolidierung zu zahlen bereit sind.

Insbesondere die letztgenannte Anforderung schließt ein massives Aufbohren von WAN-Kapazität zum Erreichen eines LAN-ähnlichen Zustandes aus. Die auf wenige Standorte konzentrierte IT kann nicht 1:1 der IT vor der Konsolidierung entsprechen. Es ist davon auszugehen, dass den Anwendungen im WAN, noch dazu in einem internationalen, erheblich weniger Bandbreite zur Verfügung steht als im LAN. Da viele Anwendungen für LAN und nicht für WAN geschrieben sind, geht jede RZ-Konsolidierung mit Änderungen im Profil der Anwendungen, in der Arbeitsteilung zwischen Clients und Servern, im Speicherkonzept und in weiteren wesentlichen Eigenschaften der Applikationen ein. Dabei sind Unterschiede zwischen Applikationen zu berücksichtigen, wie die nachfolgende Betrachtung zeigt.

Web-Anwendungen im WAN

Die Welt wäre für die Planer von RZ-Konsolidierungsmaßnahmen viel einfacher, wenn die Unternehmensapplikationen nur aus Web-Anwendungen bestünden, denn:

- Das Protokoll HTTP und die Web-Sprache HTML wurden vom Anfang an dafür entwickelt, über „dünne" Leitungen so optimal wie möglich zu funktionieren.
- Proxies, Caches, Load Balancer und dergleichen mehr sind für Web-Anwendungen verfügbar und können helfen, die Performance solcher Applikationen über das WAN wesentlich zu verbessern.

Selbst wenn auf den Einsatz von Hilfsmitteln wie Proxies und Caches verzichtet wird, zeichnen sich Webanwendungen dadurch aus, dass sie schon zu einem hohen Maß WAN-optimiert sind. Die folgenden Beispiele untermauern diese Aussage.

In einem von ComConsult durchgeführten Test, bei dem sowohl Browser als auch der Webserver im selben LAN aufgestellt waren, auf dem Browser unmittelbar vorher alle Offline-Inhalte (lokaler Cache) gelöscht worden waren und der Browser unter Umgehung jeglicher Proxies auf den Webserver zugriff, wurde beim Download der Startseite ein Durchsatz von 85.280 Bytes pro Sekunde erzielt. Dabei war die Signallaufzeit (Round Trip Time, RTT) zwischen Browser und dem sonst nicht belasteten Server kaum messbar (weit unter einer Millisekunde).

In einem zweiten Test wurde vom Browser aus über ein nationales WAN mit einer Signalumlaufzeit von ca. 100 ms auf einen Webserver zugegriffen. Dabei wurde ein Durchsatz von 17.507 Bytes pro Sekunde erzielt.

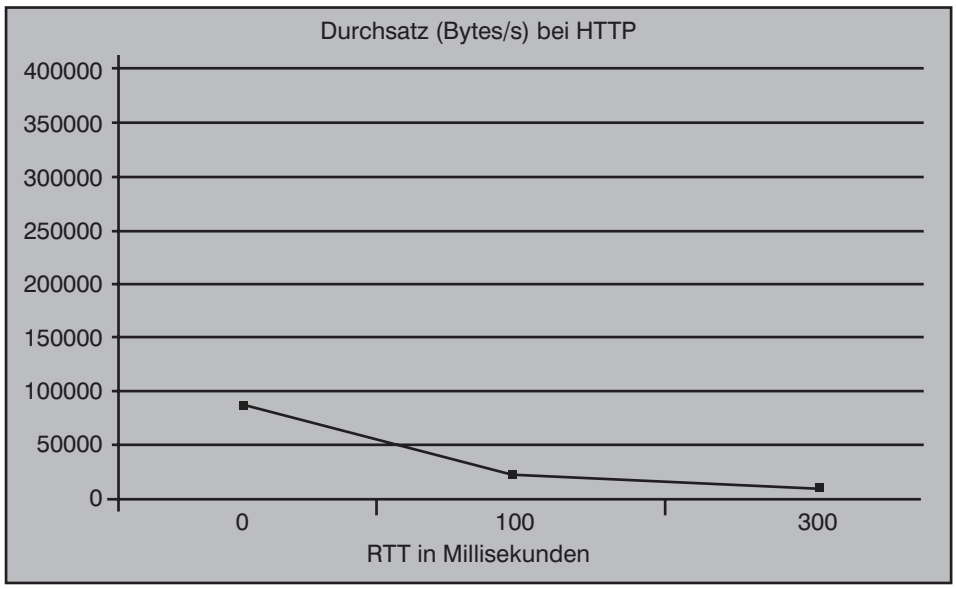


Abbildung 1

Der dritte Test wurde in einem internationalen WAN mit einer Signalumlaufzeit von ca. 300 ms und ansonsten gleichen Bedingungen durchgeführt. Der erzielte Durchsatz betrug 9.890 Bytes pro Sekunde.

Die Abhängigkeit des Durchsatzes von der Signalumlaufzeit ist in Abbildung 1 dargestellt.

Der geringere Durchsatz bei längeren Entfernungen ist plausibel, da der Datentransfer mit Handshakes, Bestätigungen und sonstigen Vorgängen arbeitet, welche eine Interaktion der beteiligten Endpunkte (Client und Server) erfordern.

Zwar ist der erzielbare Durchsatz eindeutig abhängig von der durch die geografische Entfernung verursachten Signallaufzeit, aber bei einer Verdreifachung dieses Delay-Wertes wird der Durchsatz um weniger als 50 % reduziert. Arbeitet man mit einem HTTP Cache am Standort des Browsers, ergeben sich die in Abbildung 2 dargestellten Werte für die ansonsten gleichen Randbedingungen.

Die Steigerung des Durchsatzes und damit die Verbesserung der Antwortzeit ist plausibel, weil der lokale Cache-Speicher die Zugriffszeiten zumindest für den als „Cachefähig“ markierten Teil der Webseite auf die im LAN üblichen Werte reduziert.

Auch bei Nutzung eines lokalen Caches steigt die Antwortzeit nicht linear mit der Signalumlaufzeit. Die Verdreifachung der Signalumlaufzeit reduziert die Antwortzeit der Webanwendung um weniger als 50 %.

Zwischenfazit: Webanwendungen mit und ohne Caches sind in der Regel bezüglich des Delay-Verhaltens von Netzen optimiert.

File Sharing über ein WAN

Zum Vergleich mit Webanwendungen testete ComConsult File Sharing mittels des in Windows-Netzen verbreiteten Common Internet File Service (CIFS) in einem LAN und einem WAN. Abbildung 3 zeigt die Ergebnisse bei einem Test, in dem der Inhalt eines Ordners im Windows Explorer angezeigt wurde. Der physikalische Speicherort des Ordners war auf einem Server, der Windows Explorer wurde auf einem Client ausgeführt. Im ersten Fall befanden sich beide im selben LAN, im zweiten Fall trennte die beiden ein WAN mit der Signalumlaufzeit von 40 ms.

Obwohl die RTT über das WAN lediglich 40 Millisekunden beträgt, fällt der Durchsatz auf 10 % des Durchsatzes im LAN (Vergleich: bei HTTP verursachte eine RTT von 100 ms einen Durchsatzrückgang auf 20 % im Vergleich zum LAN). Die Verzehnfachung der Antwortzeit ist nicht nur auf die niedrigere Bitrate im WAN zurückzuführen, sondern auch auf das Verkehrsprofil von CIFS, das in Abbildung 4 dargestellt ist.

Die Paketfolge zeigt, dass sich Client (NB081BM) und Server (CCBPSRV11) sehr häufig als Sender bzw. Empfänger abwechseln. Das Profil ist sehr interaktiv in dem Sinne, dass die Kommunikationspartner immer wieder (im obigen Beispiel bei jedem zweiten Paket) auf die Antwort der Gegenseite warten müssen. Dies verursacht insgesamt eine lange Wartezeit, weil sich jedes Mal die lange Signalumlaufzeit voll auswirkt. Hinzu kommt, dass herkömmliche Werkzeuge wie der Windows Explorer viel Overhead erzeugen.

Zwischenfazit: Das in Windows-Netzen für File Sharing eingesetzte Protokoll CIFS arbeitet in einem WAN nicht optimal.

Drucken über das WAN

Die Probleme mit Drucken über WAN-Leitungen niedriger Bitrate sind allgemein bekannt. Wenn man beispielsweise ein Bild ausdruckt, wird die in Formaten wie JPEG stark komprimierte grafische Information in Pixeldaten konvertiert, bevor sie zum Drucker geschickt wird. Diese letzte

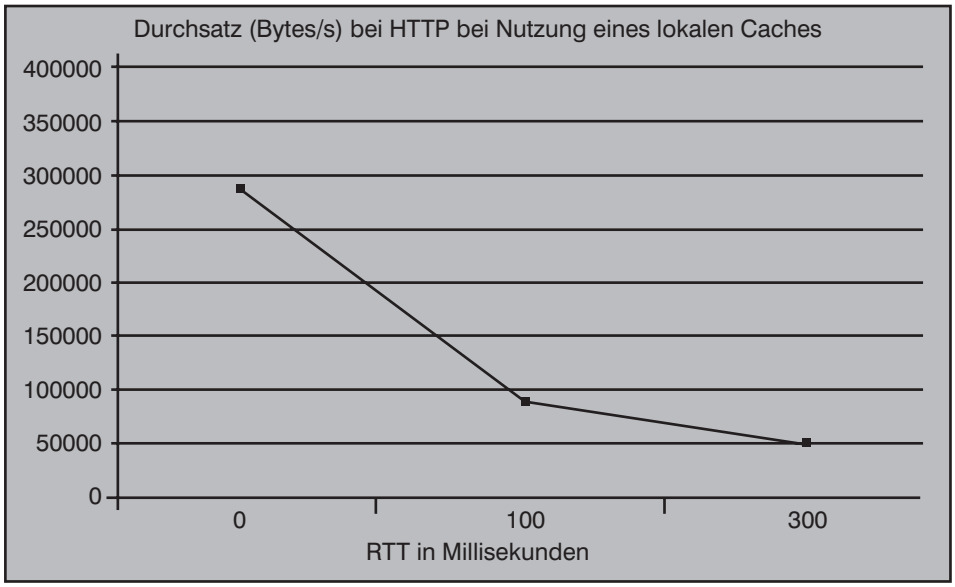


Abbildung 2

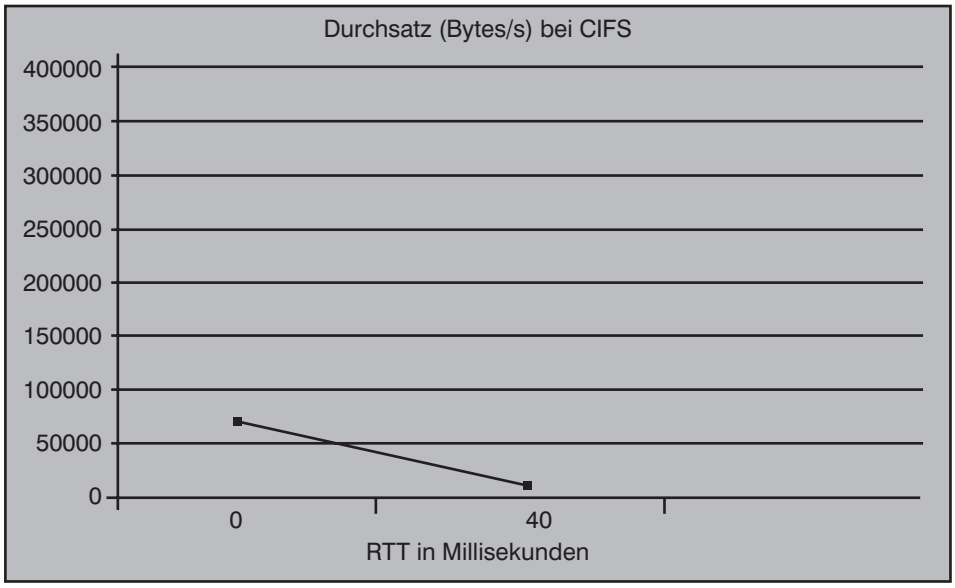
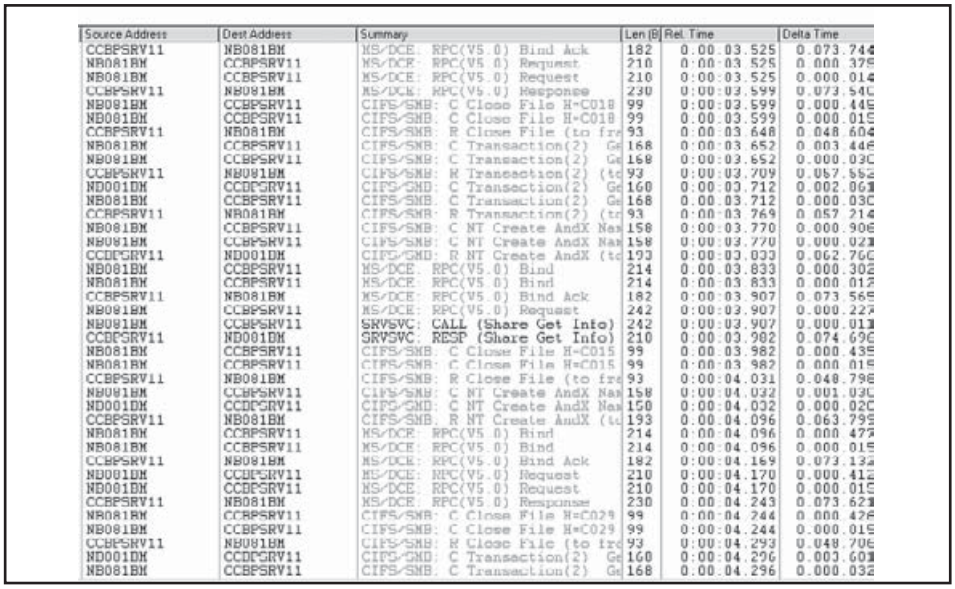


Abbildung 3



Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time
CCBPSRV11	NB081BM	MS/DCE: RPC(V5.0) Bind Ack	182	0:00:03.525	0.073.744
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Request	210	0:00:03.525	0.000.379
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Request	210	0:00:03.525	0.000.014
CCBPSRV11	NB081BM	MS/DCE: RPC(V5.0) Response	230	0:00:03.599	0.073.540
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C018	99	0:00:03.599	0.000.445
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C018	99	0:00:03.599	0.000.015
CCBPSRV11	NB081BM	CIFS/SMB: R Close File (to fra	93	0:00:03.648	0.048.604
NB081BM	CCBPSRV11	CIFS/SMB: C Transaction(2) Ge	168	0:00:03.652	0.003.446
NB081BM	CCBPSRV11	CIFS/SMB: C Transaction(2) Ge	168	0:00:03.652	0.000.030
CCBPSRV11	NB081BM	CIFS/SMB: R Transaction(2) (to	93	0:00:03.709	0.057.562
ND001DM	CCDPSRV11	CIFS/SMB: C Transaction(2) Ge	160	0:00:03.712	0.002.061
NB081BM	CCBPSRV11	CIFS/SMB: C Transaction(2) Ge	168	0:00:03.712	0.000.030
CCBPSRV11	NB081BM	CIFS/SMB: R Transaction(2) (to	93	0:00:03.769	0.057.214
NB081BM	CCBPSRV11	CIFS/SMB: C NT Create AndX Nam	158	0:00:03.770	0.000.906
NB081BM	CCBPSRV11	CIFS/SMB: C NT Create AndX Nam	158	0:00:03.770	0.000.021
CCDPSRV11	ND001DM	CIFS/SMB: R NT Create AndX (to	193	0:00:03.833	0.062.760
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Bind	214	0:00:03.833	0.000.302
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Bind	214	0:00:03.833	0.000.012
CCBPSRV11	NB081BM	MS/DCE: RPC(V5.0) Bind Ack	182	0:00:03.907	0.073.569
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Request	242	0:00:03.907	0.000.227
NB081BM	CCBPSRV11	SRVSVC: CALL (Share Get Info)	242	0:00:03.907	0.000.011
CCDPSRV11	ND001DM	SRVSVC: RESP (Share Get Info)	210	0:00:03.982	0.074.696
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C015	99	0:00:03.982	0.000.435
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C015	99	0:00:03.982	0.000.015
CCBPSRV11	NB081BM	CIFS/SMB: R Close File (to fra	93	0:00:04.031	0.048.796
NB081BM	CCBPSRV11	CIFS/SMB: C NT Create AndX Nam	158	0:00:04.032	0.001.030
ND001DM	CCDPSRV11	CIFS/SMB: C NT Create AndX Nam	150	0:00:04.032	0.000.020
CCBPSRV11	NB081BM	CIFS/SMB: R NT Create AndX (to	193	0:00:04.096	0.063.795
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Bind	214	0:00:04.096	0.000.472
NB081BM	CCBPSRV11	MS/DCE: RPC(V5.0) Bind	214	0:00:04.096	0.000.015
CCBPSRV11	NB081BM	MS/DCE: RPC(V5.0) Bind Ack	182	0:00:04.169	0.073.132
ND001DM	CCDPSRV11	MS/DCE: RPC(V5.0) Request	210	0:00:04.170	0.000.412
ND001DM	CCDPSRV11	MS/DCE: RPC(V5.0) Request	210	0:00:04.170	0.000.015
CCBPSRV11	NB081BM	MS/DCE: RPC(V5.0) Response	230	0:00:04.243	0.073.621
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C029	99	0:00:04.244	0.000.426
NB081BM	CCBPSRV11	CIFS/SMB: C Close File H=C029	99	0:00:04.244	0.000.015
CCBPSRV11	NB081BM	CIFS/SMB: R Close File (to fra	93	0:00:04.293	0.048.706
ND001DM	CCDPSRV11	CIFS/SMB: C Transaction(2) Ge	160	0:00:04.296	0.003.601
NB081BM	CCBPSRV11	CIFS/SMB: C Transaction(2) Ge	168	0:00:04.296	0.000.032

Abbildung 4: Trace File zur CIFS-Kommunikation über ein WAN

Teilstrecke der Reise von der Anwendung zum Drucker muss in der Regel um Größenordnungen mehr Informationen übertragen als zum Beispiel das Segment zwischen einem Client und einem Druckserver. Daher sollten Drucker möglichst nicht über WAN angesteuert werden. Teilweise ist dies jedoch nicht zu umgehen, wenn zum Beispiel der Benutzer einer Terminalserveranwendung auf einen Terminalserver über das WAN zugreift, aber von der Anwendung aus lokal drucken will.

Zwischenfazit: Mechanismen für die Steuerung von Druckern und Druckjobs sind in der Regel nicht WAN-optimiert.

Elektronische Post über das WAN

Viele Unternehmen haben ihre E-Mail-Server-Struktur dahingehend konsolidiert, dass wenige E-Mail-Server in Data Centern aufgestellt werden und die Clients über das WAN auf diese Server zugreifen. Sofern es sich um Web Clients handelt, gelten für diese Anwendungen die selben Aussagen wie für andere Webanwendungen. Web-basierende E-Mail Clients sind jedoch zwar WAN-optimiert, aber in der Funktionalität im Vergleich zu proprietären Clients der Hersteller von E-Mail-Systemen wie Micrsoft Exchange oder Lotus Notes eingeschränkt. So verwenden die meisten Anwender in Unternehmensnetzen die E-Mail-Client-Software der betreffenden Hersteller, allerdings mit unterschiedlichen Konfigurationen. Einige Anwender benutzen den E-Mail Client lediglich zum Zugriff auf die E-Mail-Datenbank, die ausschließlich auf dem Server verweilt. Andere stoßen Replikationen zwischen der Serverbasierenden Datenbank und einer lokalen Datenbank des Clients an.
Je nach Konfiguration des E-Mail Clients werden im WAN unterschiedliche Performance-Erfahrungen gemacht. Die WAN-freundlichste Konfiguration besteht darin, auf automatische Replikationen zu verzichten und eine Information aus der elektronischen Post nur dann herunterzuladen, wenn es erforderlich ist. Aber selbst bei einer solchen Konfiguration sind die Anwender vor Überraschungen nicht gefeit. ComConsult stellte beispielsweise fest, dass bei Nutzung der Virenschutzoption von Lotus Notes der Anhang einer Nachricht auch beim bloßen Sichten der Nachricht zum Client übertragen wurde. Anwender haben sich dabei gewundert, warum das reine Öffnen der Nachricht so lange dauerte, wenn der Client über ein WAN auf den Notes-Server zugriff.

Zwischenfazit: Das Verhalten von E-Mail im WAN variiert ganz stark mit dem Profil und den Einstellungen für E-Mail. Das WAN-freundlichste Verhalten wird in der Regel durch Verzicht auf automatische Replikationen erzielt.

Kompression im WAN

Ein Ansatz, die Leistungsfähigkeit des WAN zu erhöhen, ist die Nutzung von Kompression. Module in WAN-Routern oder Appliances, die diesen Routern vorgeschaltet werden, können die über das WAN übertragene Datenmenge durch Anwendung diverser Kompressionsverfahren reduzieren. Entscheidend ist dabei, ob sich das WAN-Verkehrsprofil für die Anwendung der Datenreduzierungsverfahren eignet. ComConsult stellte in Tests beispielsweise fest, dass Verfahren, die auf der Erkennung von wiederholten Datensequenzen basieren, unter bestimmten Bedingungen, welche die Grenzen der Appliances ausreizen, wie z. B. der Übertragung von sehr großen Dateien, ihre Wirksamkeit verlieren. Abbildung 5 zeigt beispielsweise den Vergleich zwischen den gemessenen Zeiten für die Übertragung einer 200 MB großen

Datei über eine WAN-Leitung mit der Übertragungsrate 4 Mbit/s, wobei den WAN-Routern Appliances des Herstellers Peribit vorgeschaltet waren. Die Kompression ist unter diesen Umständen nicht wirksam. Ohne Kompression dauert die Übertragung ca. 430 Sekunden, mit Kompression sogar mehr (480 Sekunden), weil die Verarbeitung durch die Appliances Zeit in Anspruch nimmt. Der erste Versuch mit Kompression weist sogar eine wesentlich längere Übertragungsdauer (ca. 680 Sekunden) auf. Erst nach der Erkennung von wiederholten Sequenzen durch die Appliances sinkt die Übertragungsdauer auf 480 Sekunden, aber nicht auf die ohne Kompression erreichten 430 Sekunden.

Dagegen zeigt Abbildung 6, dass bei einer Dateigröße von 20 MB und einer WAN-Bitrate von 2 Mbit/s bereits eine wesentliche Kompression durch die Appliances erzielt werden kann. Statt über 100 Sekunden braucht man für den File Transfer nach einigen Wiederholungen (welche die Erkennung wiederholter Sequenzen durch die Appliances bewirken) weniger als 40 Sekunden.

Noch bessere Ergebnisse wurden bei Leitungen niedrigerer Bitrate und kleineren Dateien erzielt. Die beste Wirkung hatten die Kompressoren bei HTTP. Zwar sind bei HTTP alternativ zur WAN-Kompression Web Caches einsetzbar, aber ein Unternehmen, das die Web Proxies auf einen Standort konzentriert und an anderen Standorten keine solchen Proxies mehr unterhält, kann mittels WAN-Kompression die Kommunikation zwischen Web Clients und Web Proxies über ein WAN wesentlich beschleunigen.

Zwischenfazit: Je nach Applikationsprofil und WAN-Bitraten kann Kompression ein vielversprechender Ansatz für die Erhöhung der Leistungsfähigkeit von WAN sein. Aber dieser Ansatz bringt nicht für alle Anwendungsfälle die gewünschten Ergebnisse. Vor der Implementierung von WAN-Kompression sind Tests auf jeden Fall zu empfehlen.

Lösungen für File Sharing

WAN-Kompression ist ein Verfahren, das ohne Rücksicht auf die Besonderheiten von Anwendungen die über WAN-Leitungen niedriger Bitrate übertragene Datenmenge zu reduzieren versucht. Von einem solchen Verfahren profitieren potenziell alle Anwendungen, aber diese Methode lässt die Besonderheiten von Anwendungen unberücksichtigt. Als Alternative zu WAN-Kompression sind Verfahren verfügbar, welche die Leistungssteigerung speziell für bestimmte Anwendungen ermöglichen. Spezielle Optimierungsansätze für Webverkehr wurden bereits erwähnt (beispielsweise Caches). Analog sind mittlerweile Mechanismen für die Optimierung von File Sharing über WAN verfügbar.

Eine Methode, bekannt als Web File Store, nutzt Webserver als File Server. Dabei nutzen die Anwender statt herkömmlicher Werkzeuge wie Windows Explorer eine Weboberfläche für File Sharing.

Eine Methode für File Sharing mittels Web ist als WebDAV (Web-based Distributed Authoring and Versioning) bekannt. Durch Ergänzungen des HTTP-Protokolls werden Möglichkeiten geschaffen, dass Benutzer gemeinsam Dateien auf Webservern verwalten und editieren. Ursprünglich für das Management von Web-Seiten entwickelt, ist aus DAV bzw. WebDAV eine Art netzbasierendes Dateisystem mit spezieller Eignung für Netze mit hoher Latenzzeit geworden. Die wichtigsten Funktionen von WebDAV sind:

- File Locking zur Wahrung der Konsistenz von Daten durch Verhinderung gleichzeitiger Schreibzugriffe
- Werkzeuge für die Indizierung und die Suche in DAV-Ordnern
- Erstellung, Kopieren und Verlagerung von Ordnern

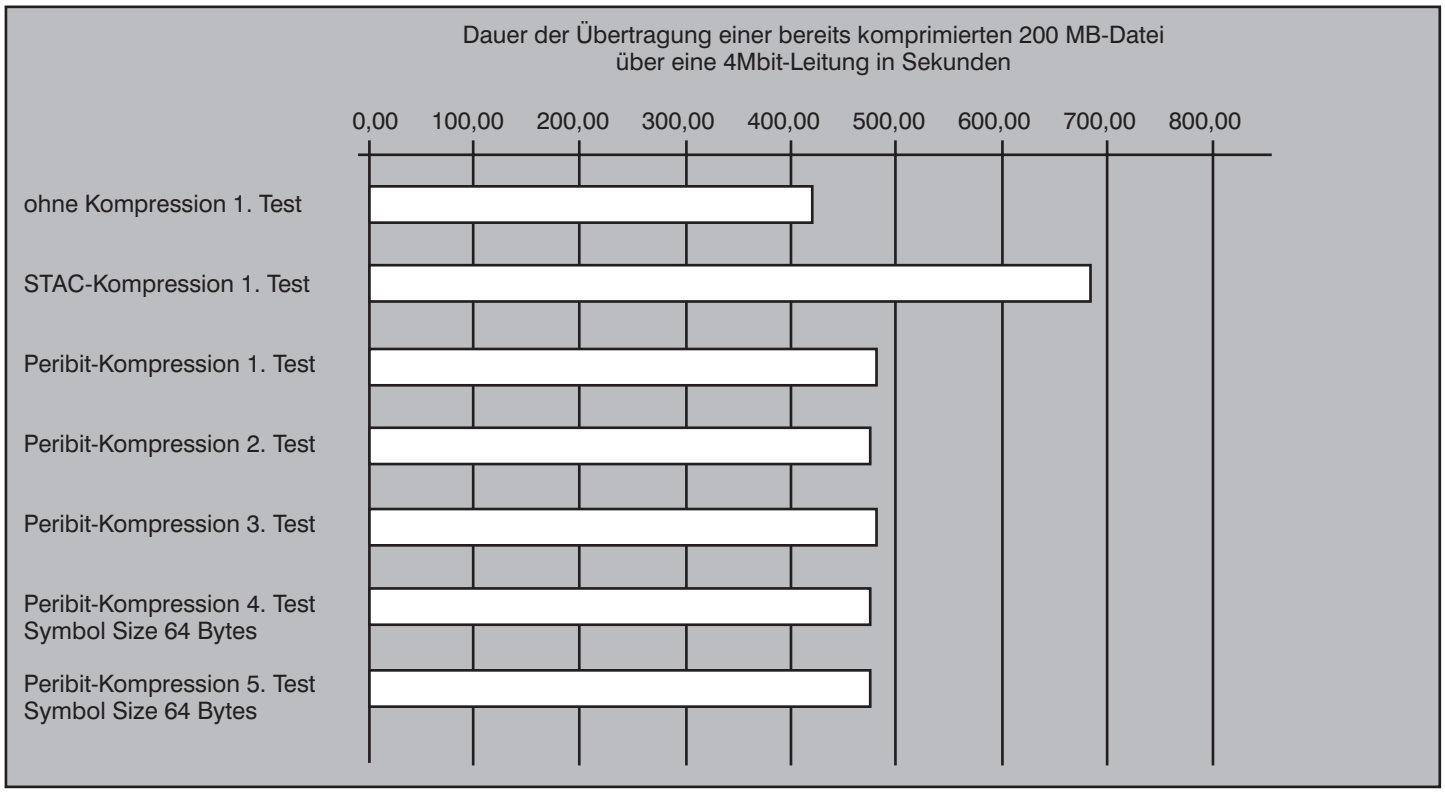


Abbildung 5

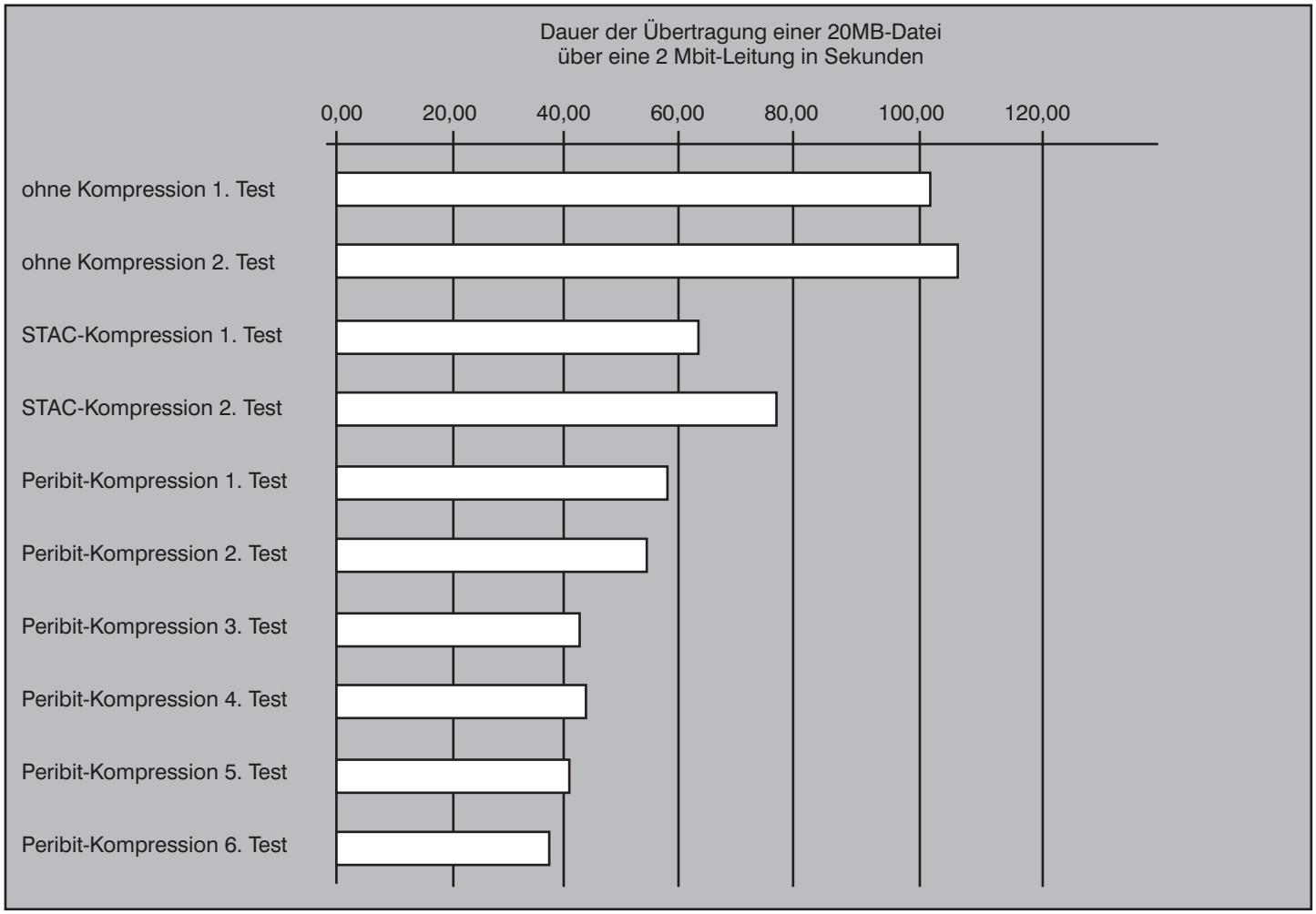


Abbildung 6

Die wichtigsten Standards im Zusammenhang mit WebDAV sind die folgenden Requests for Comments:

- RFC 2518 unter dem Titel HTTP Extensions for Distributed Authoring: In der Entwicklung des Standards waren Microsoft, Netscape und Novell beteiligt. Darin werden die Mechanismen für File Locking, Namensverwaltung, Beschreibung der Dateieigenschaften etc. beschrieben.

- RFC 3253 unter dem Titel Versioning Extensions to WebDAV: Dieser Standard wurde u. a. von IBM und Microsoft entwickelt.

- RFC 3648 unter dem Titel Web Distributed Authoring and Versioning (WebDAV) Ordered Collections Protocol: Collections sind im WebDAV-Jargon die Ordner, welche die Dateien enthalten.

- RFC 3744 unter dem Titel Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol: Unter Mitwirkung von u. a. IBM und Oracle beschreibt dieses Dokument die Methoden für die Verwaltung von Berechtigungen in einem WebDAV-Umfeld.

Ein Beispiel für eine WebDAV-Implementierung ist der WebFile Server (WFS) vom Hersteller Xythos.

Zwar werden mit solchen Methoden einige Overheads und das suboptimale Verhalten des herkömmlichen File Sharing vermieden, aber das eigentliche Problem, dass der File Transfer über das WAN die WAN-Kapazität zu einem Großteil belegt, wird nicht gelöst. Ein weiterer Nachteil kann je nach Produkt in der Administration liegen. Die Verwaltung von Berechtigungen bei File Sharing erfolgt mittlerweile in den meisten Unternehmen mittels zentral gesteuerter Werkzeuge wie Microsoft Active Directory. Bei Einsatz von Web File Stores stellt sich immer die Frage, ob die Berechtigungen managebar bleiben.

Anders als Web File Stores arbeiten Dateisynchronisationsverfahren derart, dass die zentral verwalteten Informationen eines File Servers über das WAN repliziert werden. Wird eine Datei geändert, und nur dann, erfolgt das Kopieren auf die Träger von Replika der Datei. File Locking muss in diesem Fall auch über das WAN funktionieren, d. h. der schreibende Zugriff eines Benutzers (mit der entsprechenden Berechtigung) auf eine Kopie der Datei muss bewirken, dass kein schreibender Zugriff auf eine andere Kopie der Datei (auch an anderen Standorten) mehr möglich ist, solange die Datei vom ersten Benutzer bearbeitet wird.

Ein Beispiel für solche Replikationsmethoden ist der Ansatz Wide Area File Services (WAFS) von Cisco Systems. WAFS wird von den so genannten File Engines des Herstellers unterstützt. Eine typische Konstellation ist in Abbildung 7 dargestellt.

Dabei sind die in den peripheren Standorten installierten Edge File Engines (Edge

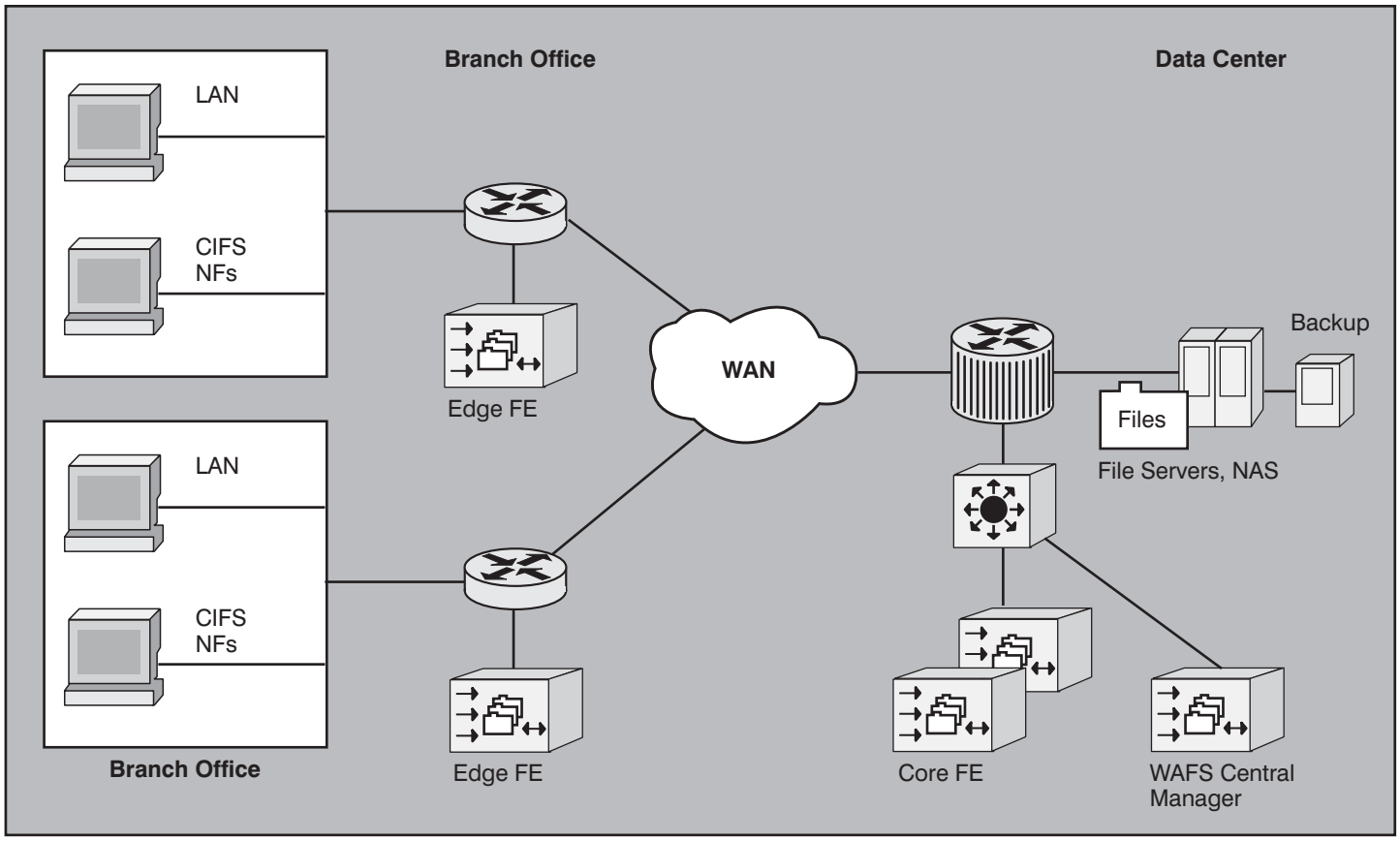


Abbildung 7: Wide Area File Services (WAFS) von Cisco

FE) als Ersatz für lokale File und Print Server gedacht und halten lokale Kopien der zentral auf einem Fileserver oder Network Attached Storage (NAS) verwalteten Dateien. Am zentralen Standort wird ein Core FE aufgestellt, der die Requests der Edge FE entgegennimmt und bearbeitet. Dabei kommuniziert der Core FE direkt mit dem zentralen Fileserver bzw. NAS. Die Funktion des Core FE besteht vor allem darin, die weniger WAN-optimierten Protokolle CIFS und NFS (Network File System) in eine Form umzuwandeln, die WAN-tauglich ist. Dieses optimale WAN-Profil wird bei der Kommunikation zwischen Core und Edge FE verwendet. Die Verwaltung der File Engines obliegt dem so genannten WAFS Control Manager.

Problematisch sind File-Synchronisationsansätze bei Offline-Kopien. Das Verfahren Dateisynchronisation funktioniert nur bei Aufrechterhaltung einer Verbindung zwischen den Trägern des Originals und der Kopien der Daten.

Wird z. B. die Datei auf die Festplatte eines Notebooks kopiert, dessen Benutzer die Datei auch dann bearbeitet, wenn er über keine Online-Verbindung zum Unternehmensnetz verfügt, kann File Locking nicht mehr verhindern, dass die Konsistenz der Datei durch gleichzeitige Modifikationen der Originalversion durch verschiedene Benutzer verloren geht.

Explodierende E-Mail-Datenbanken

Mangels brauchbarer Verfahren für File Sharing über WAN hat sich E-Mail als Methode für den Austausch von Dateien in vielen Unternehmen etabliert. Da die Benutzung eines zentralen Fileservers mittels Zugriffe über das WAN bisher keine akzeptablen Antwortzeiten bietet, greifen die Anwender zum bequemen E-Mail-System und tauschen Nachrichten aus, die als Anhang Dateien enthalten.

Mit zunehmenden grafischen und sogar akustischen und Video-Informationen in Dateien explodieren somit die Datenmengen in den E-Mail-Datenbanken. Neben dem Fileserver, dem eigentlichen Aufbewahrungsort der Datei, taucht diese in der Datenbank des E-Mail-Systems noch einmal auf, bei einer Mehrzahl von Empfängern gleich mehrfach. Es entstehen dabei viele Probleme:

- Die verschiedenen Kopien der Datei auf dem Fileserver und in der Mail-Datenbank sind miteinander nicht synchronisiert. Die Konsistenz der Datei kann verloren gehen, da verschiedene Kopien der Datei gleichzeitig bearbeitet werden können.
- Die WAN-Bitrate wird mehrfach belegt, indem jeder Empfänger eine Kopie der Datei erhält.
- Die Kosten für Storage steigen durch die Mehrfachspeicherung der Daten und die erforderliche Sicherung aller Kopien.
- Die Datenbanken der E-Mail-Systeme wachsen mit sehr hohem Tempo. ComConsult sind aus eigenen diversen Troubleshooting-Einsätzen Probleme bekannt, die auf das unkontrollierte Wachstum von E-Mail-Datenbanken zurückzuführen sind. Die Gefahr, dass unter solchen Bedingungen Datenbankprobleme entstehen, wächst. Entstehen Defekte in einer sehr großen Datenbank, ist die Reparatur sehr schwierig.

Zwischenfazit: Die mit explodierenden E-Mail-Datenbanken verbundenen Probleme können nur gelöst werden, wenn den Anwendern eine akzeptable Alternative zum

8515	459	[10.10.230.25]	[10.10.240.58]	282	TNS	Continuation of frame 3950; 228 Bytes of data
8516	1032	[10.10.240.58]	[10.10.230.25]	124	TNS	Continuation of frame 5321; 70 Bytes of data
8517	351	[10.10.230.25]	[10.10.240.58]	88	TNS	Continuation of frame 3950; 34 Bytes of data
8518	871	[10.10.240.58]	[10.10.230.25]	118	TNS	Continuation of frame 5321; 64 Bytes of data
8519	65	[10.10.230.25]	[10.10.240.58]	159	TNS	Continuation of frame 3950; 105 Bytes of data
8520	1050	[10.10.240.58]	[10.10.230.25]	135	TNS	Continuation of frame 5321; 81 Bytes of data
8521	82	[10.10.230.25]	[10.10.240.58]	75	TNS	Continuation of frame 3950; 21 Bytes of data
8522	1315	[10.10.240.58]	[10.10.230.25]	150	TNS	Continuation of frame 5321; 96 Bytes of data
8523	454	[10.10.230.25]	[10.10.240.58]	283	TNS	Continuation of frame 3950; 229 Bytes of data
8524	1093	[10.10.240.58]	[10.10.230.25]	124	TNS	Continuation of frame 5321; 70 Bytes of data
8525	215	[10.10.230.25]	[10.10.240.58]	79	TNS	Continuation of frame 3950; 25 Bytes of data
8526	2487	[10.10.240.58]	[10.10.230.25]	138	TNS	Continuation of frame 5321; 84 Bytes of data
8527	398	[10.10.230.25]	[10.10.240.58]	256	TNS	Continuation of frame 3950; 202 Bytes of data
8528	1009	[10.10.240.58]	[10.10.230.25]	124	TNS	Continuation of frame 5321; 70 Bytes of data
8529	297	[10.10.230.25]	[10.10.240.58]	88	TNS	Continuation of frame 3950; 34 Bytes of data
8530	723	[10.10.240.58]	[10.10.230.25]	118	TNS	Continuation of frame 5321; 64 Bytes of data
8531	93	[10.10.230.25]	[10.10.240.58]	159	TNS	Continuation of frame 3950; 105 Bytes of data
8532	954	[10.10.240.58]	[10.10.230.25]	135	TNS	Continuation of frame 5321; 81 Bytes of data
8533	297	[10.10.230.25]	[10.10.240.58]	75	TNS	Continuation of frame 3950; 21 Bytes of data
8534	1241	[10.10.240.58]	[10.10.230.25]	194	TNS	Continuation of frame 5321; 140 Bytes of data

Tabelle 1

Missbrauch von E-Mail für Dateiaustausch geboten wird. Werkzeuge für File Sharing können als eine solche Alternative dienen. Diese Werkzeuge lösen jedoch nicht das Problem der Synchronisation mit Offline-Benutzern, wobei dieses Problem auch dann besteht, wenn E-Mail als Medium für File Sharing benutzt wird.

Datenbankzugriffe über das WAN

Ein Problem, das weder von WAN-Kompression noch von File-Replikation gelöst wird, besteht in den Schwierigkeiten, über das WAN auf Datenbanken zuzugreifen. Viele Benutzer von Datenbankapplikationen haben die Erfahrung gemacht, dass solche Applikationen zwar im LAN, jedoch nicht im WAN mit akzeptablen Antwortzeiten funktionieren. Dabei ist weniger die Bitrate des WAN, sondern die durch lange Entfernungen verursachte Signallaufzeit das Problem.

Die nähere Analyse des Lastprofils von Datenbankapplikationen mit Fat Clients durch ComConsult hat ergeben, dass bei Nutzung von Protokollen wie Transparent Network Substrate (TNS) bzw. SQL.net zu den wichtigsten Merkmalen des Lastprofils der Umstand gehört, dass der Server auf ein Paket des Clients mit einem Paket reagiert und umgekehrt. D. h. ein „Bursting“ in dem Sinne, dass der Server eine Anfrage mit der Übermittlung einer ununterbrochenen Folge von Paketen beantwortet, findet nicht statt. Ein Beispiel für eine solche Kommunikation ist in Tabelle 1 dargestellt.

Server und Client wechseln sich als Sender bzw. Empfänger ständig ab. Für jedes Paketpaar ist als Übertragungszeit die volle Round Trip Time (RTT) zwischen Client und Server zu berücksichtigen. Werden so z. B. 4.000 Pakete vom Server zum Client und vom Client zum Server übertragen, entsteht eine Gesamtlatenz von 4.000*RTT bzw. 8.000*OneWayDelay.

Ein solches Kommunikationsprofil ist dann besonders problematisch, wenn der Delay im Netz (Signalverzögerung) steigt. Für den obigen Paketaustausch (gemessen in einem produktiven Netz) mit insgesamt 8.515 Paketen berechnete ComConsult das Verhältnis zwischen der Antwortzeit über eine längere Strecke zwischen Client und Server im Verhältnis zur Antwortzeit im LAN-Szenario. Dieses als „Antwortzeitfaktor“ in Abhängigkeit von der Entfernung berechnete Verhältnis ist in Abbildung 8 dargestellt.

Obwohl selbst die intensive Arbeit mit einer Datenbankanwendung verhältnismäßig geringe Netzlasten von wenigen Mbit/s in der Summe beider Richtungen verursacht, ist bei WAN-Anbindungen von wesentlich längeren Antwortzeiten im Vergleich zur rein LAN-basierenden Übertragung auszugehen.

Die Schlussfolgerungen für die Arbeit mit Fat Clients für den Zugriff auf Datenbanken sind wie folgt:

- Die anzusetzende Mindestbitrate für eine Anbindung beträgt aufgrund des Delay-Verhaltens der Anwendung 2 Mbit/s, denn bei niedrigeren Bitraten würde die für die Bildung von Paketen auf der WAN-Strecke benötigten Zeit das Antwortzeitverhalten der Anwendung zu sehr belasten.

- Das Kommunikationsprofil zwischen Fat Client und Server ist nur bis zu einem Kabelweg von 200 km WAN-tauglich.

- Wenn die Datenbankanwendung mit einem wiederholten „Nachladen“ von Daten vom Server auf den Client arbeitet, ist aufgrund der hohen Datenmengen, die durch Nachladen von Dateien übertragen werden, dafür zu sorgen, dass lokale Caches dieses Nachladen überflüssig machen.

Eine Steigerung der Effizienz von Datenbankanwendungen im WAN ist dadurch

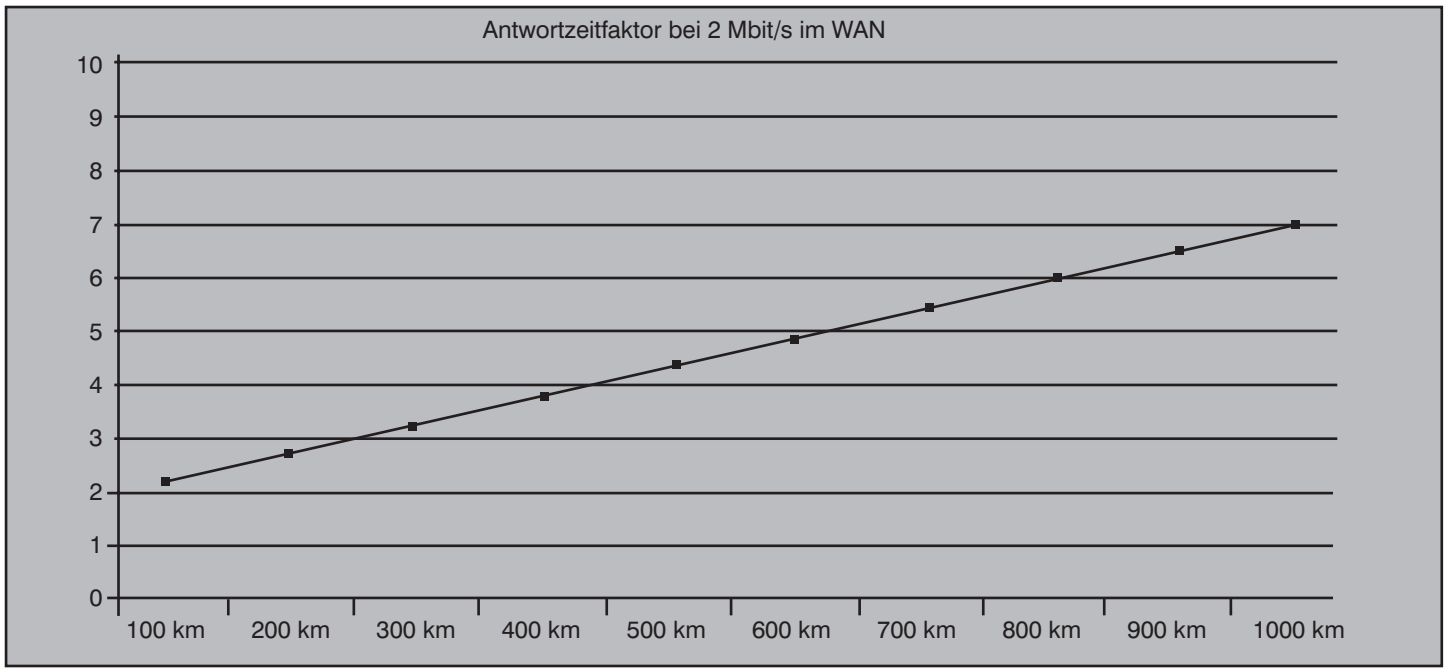


Abbildung 8: Antwortzeit einer Datenbank, abhängig von der Entfernung zwischen Fat Client und Server

zu erreichen, dass eine zusätzliche Ebene in der Anwendungsarchitektur zwischen Client und Server vorgesehen wird. Wenn die Datenbankapplikation statt auf dem Arbeitsplatzrechner auf einem Rechner in unmittelbarer Nähe des Datenbankservers läuft, wird die Effizienz der Anwendung wesentlich gesteigert. Dies kann entweder dadurch erreicht werden, dass die Applikation auf einem Terminalserver residiert, auf den von den Arbeitsplätzen aus per Terminalclient zugegriffen wird, oder dadurch, dass von Web-Browsern aus auf die Applikation zugegriffen wird. Die Applikation läuft im zweiten Fall auf einem Applikationsserver in unmittelbarer Nähe des Datenbankservers. In der Regel wird eine Kommunikationskette nach dem Schema Browser – Webserver – Applikationsserver – Datenbankserver realisiert. Java Front Ends oder ähnliche Technologien können dabei helfen, trotz Thin Clients auch komplexe Anwendungen zu entwickeln.

Collaboration über das WAN

Unter dem Stichwort „Collaboration“ kann man alle IT-Anwendungen zusammenfassen, die eine enge Zusammenarbeit zwischen Anwendern an entfernten Standorten ermöglichen. Das einleuchtendste Beispiel sind herkömmliche Telefonate oder Telefonkonferenzen. Viele Geschäftsprozesse basieren auf solchen Kommunikationsbeziehungen mittels des herkömmlichen Telefons. Um die Telefonie mit zusätzlichen nützlichen Funktionen wie Wählen aus Verzeichnissen, Konferenzen, Rückruf bei besetzt etc. zu versehen, haben viele Unternehmen Verbünde aus Telefonanlagen aufgebaut, die sich auf Standorte im ganzen Land oder gar in verschiedenen Ländern erstrecken.

Weitere Beispiele für Collaboration sind Videokonferenzen (die mittlerweile nicht nur mit ISDN-basierenden Studiosystemen, sondern auch mit Desktopsystemen und IP-basierend funktionieren), Messaging-Systeme, Application Sharing, unter dem Schlagwort „Presence-based“ bekannten Anwendungen etc.

Auch solche Anwendungen unterliegen zurzeit dem Konsolidierungstrend. Wenn beispielsweise Voice over IP (VoIP) mit dem „Diktat der Geografie“ aufräumt und ermöglicht, dass ein IP-Telefon in Tokio an einen Call Processing Server in

Frankfurt angebunden ist, dann kann man zentrale Ressourcen einer Voice-Infrastruktur auf wenige Data Center konzentrieren. Erstens werden damit Kosten gespart, und zweitens kann man Leistungsmerkmale nutzen, die bislang aufgrund technischer Barrieren zwischen TK-Anlagen an verschiedenen Standorten nicht realisierbar waren.

Aber das Leben wäre zu einfach, wenn es hierbei keine zu lösenden Probleme gäbe. Einige Beispiele für solche Probleme sind wie folgt:

- Wenn man das Leistungsmerkmal „music on hold“ nutzt, hört ein Teilnehmer, dessen Gespräch mit einem Kommunikationspartner „gehalten“ wird, häufig eine Musik, die von der TK-Anlage kommt. Wird ein Gespräch zwischen zwei Teilnehmern in Tokio gehalten, würde eine solche Musik Bandbreite zwischen Frankfurt und Tokio belegen, wenn es dafür in Tokio keine Quelle gibt (wenn die Umgebung in Tokio nur aus IP-Telefonen besteht).

- Wenn mehrere Teilnehmer in Tokio eine Telefonkonferenz abhalten und es dort keinen Konferenzserver gibt, muss zwischen dem Konferenzserver in Frankfurt und jedem Teilnehmer in Tokio ein Voice-Kanal eingerichtet werden.

- Wenn ein Teilnehmer in Tokio den Notruf wählt, kann er bei fehlenden Vorkehrungen dagegen mit der Notrufzentrale in Frankfurt verbunden werden.

Völlig ohne lokale Service-Instanzen in Tokio kommt man also nicht aus. Solche Instanzen können beispielsweise auf einem Gateways residieren, der die folgenden Funktionen bietet:

- Lokaler „Amtskopf“ für kommende und gehende Gespräche, damit lokale Telefonate nicht mit internationalen Tarifen bezahlt werden und der lokale Notruf funktioniert

- „Abgespeckte“ Serverfunktionalität für den Fall, dass die WAN-Verbindung zum Data Center unterbrochen wird und die lokalen Endgeräte weiterhin Call Processing Services nutzen müssen

- Konferenzdienste für lokale Konferenzen

- Quelle für „music on hold“

Solche lokale Instanzen ergänzen die zentrale und konsolidierte Call Processing Infrastruktur, die auf wenigen Servern in wenigen Data Centern basieren kann und Funktionen wie weltweite Verzeichnisse, zentrales Management von Benutzern, standortübergreifende Nutzung von modernen Kommunikationsdiensten wie Unified Messaging, Collaboration, Presence etc. bietet.

Fazit

Der Trend zur Konsolidierung von IT-Diensten durch Konzentration von Servern auf wenige Data Center stellt die Planer der Infrastruktur und der Dienste vor neue technische Herausforderungen, von der Optimierung des Antwortzeitverhaltens der Anwendungen im WAN bis zur Lösung spezifischer Probleme im Zusammenhang mit Voice. Diese Probleme sind jedoch lösbar. Moderne Werkzeuge und Mechanismen für die Lösung dieser Probleme sind verfügbar. Aber eine Konsolidierung zum Nulltarif gibt es nicht. Die Unternehmen müssen bereit sein, die notwendigen Investitionen in die Tools und Verfahren für die Lösung der Probleme zu tätigen. Unter dem Strich bleiben jedoch in vielen Fällen genügend wirtschaftliche Vorteile der RZ-Konsolidierung.

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2005

Organisation und Technik der IT-Sicherheit mit Fachanalysen und Praxis-Workshops

Vom 06. - 09. Juni 2005 veranstaltet die ComConsult Akademie ihren Sicherheits-Kongress "ComConsult IT-Sicherheits-Forum 2005" in Königswinter.

Das Programm besteht aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen. Das Forum verbindet die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Ader diesjährige Secuity-Kongress der ComConsult Akademie legt großen Wert auf Praxisnähe und bietet deshalb neben der notwendigen Behandlung ganz neuer Themen auch vielfältige Empfehlungen und direkt umsetzbare „Tipps und Tricks" für den Tagesbetrieb. Sie hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt.

An insgesamt vier Tagen werden angeboten:
- Aktuelle Übersicht zum Stand der Sicherheitsbedrohungen
- Trends und Marktentwicklungen bei Sicherheitstechnologien
- Behandlung wichtiger Bereiche der Sicherheitsorganisation
- Moderierte Produktvergleiche mit Live-Demos
- Vertiefende Tutorien und Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren, mit folgenden Themen:
- IT-Sicherheit im Überblick
  Stand und Ausblick bei wichtigen Sicherheitsthemen (Organisation und Technik)
- Sicherheit von Web-Applikationen
  Live-Hacks und Konzeption von Schutzmaßnahmen
- Information Security Management
  BS7799-1 und -2, Aufbau eines ISMS

Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle fachliche Entwicklungen und Praxisbeispiele vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu speziellen Themen vorbehalten. Da diese

parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2005 sind vorgesehen:

Endpoint Security - Dezentralisierung der Schutzmaßnahmen
- Notwendige Schutzfunktionen am Endpoint
- Anforderungen an das zentrale Management
- Endpoint Security Enforcement
- Cisco-NAC vs Microsoft-NAP

Identity Management
- IM und seine Bausteine (Directory Management, Provisioning, Access Management)
- Die Bedeutung von IM für die Sicherheitsinfrastruktur
- Wie kann man mit IM Kosten senken?
- Roadmap zur Einführung von IM

Security Management
- Problem der fehlenden Sicherheitsstandards
- Lösungen zum Security Information Management (SIM)
- Event-Aggregation und Event-Correlation
- Probleme von SIM-Tools in stark heterogenen Netzen

Sichere Nutzung von Webapplikationen
- Mit welchen Techniken werden Webapplikationen angegriffen?
- Vorstellung von Fallstudien und Erkenntnisse
- Sicherheitshinweise für Entwickler von Webapplikationen
- Sicherung von Webapplikationen mit Application Security Gateways

Was bringt die virtuelle Poststelle?
- Client- vs Server-basierte Mailverschlüsselung
- Signatur und Verschlüsselung durch zentrale Gateways (S/MIME, PGP)
- Zertifikats-Managements mit Benutzer-Domain- und Gruppenzertifikaten.
- Umsetzung von Anforderungen (BDSG, Grundschutzhandbuch BSI, BS 7799)

Sicherheitsaspekte bei Voice-over-IP
- Absehbare Bedrohungen gegen VOIP-Verbindungen
- Sicherheitsfeatures bei H.323 und SIP
- Auswirkungen der Sicherheitsinfrastruktur auf die QoS bei VOIP
- Wie kann man „Softphones" sicher betreiben?
- Physische Sicherheit in IT-Umgebun gen
- Haftungsrisiken für IT-Verantwortliche
- Sicherheit in der Bauausführung und Infrastruktur
- Sichere Ausführung von Energieversorgung, Zugangs- und Brandmeldetechnik
- Technische Sicherheit der IT-Komponenten

Schutz kritischer Datenbestände
- Disk- vs File-Encryption
- Schutz mobiler Daten: vom Notebook bis zum PDA
- wie umgehen mit „removable media"?
- Anforderungen an das zentrale Management

Aufbau eines ISMS nach BS 7799
- BS 7799 und Abgrenzung zum BSI-GSHB
- PDCA - die vier Phasen eines ISMS-Projektes
- Aufbau und Umsetzung in einer Konzernumgebung

ComConsult IT-Sicherheitsforum 2005

- Welche Fehler sollte man unbedingt vermeiden

Linux und Windows
- Ist Open Source sicherer als Closed Source?
- Kann Linux im Client -/ Server -Bereich empfohlen werden?
- Sind kombinierte Lösungen sinnvoll?

Security Awareness und Governance
- Einbeziehung der IT-Prozesse in das interne Kontrollsystem
- Bekanntmachung und Durchsetzung einer SecPol im Konzernumfeld
- Durchführung einer Security
- Awareness-Kampagne

Weitere vorgesehene Themen
- VPN: IPsec vs SSL
- SAP-Security
- IT-Revision
- Forensische Untersuchungen

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen hat einen hohen praktischen Wert für die Teilnehmer. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier nach aller Erfahrung immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

Moderator
Dipl.-Inform. Detlef Weidenhammer

ComConsult IT-Sicherheits-Forum 2005 06. - 09.06.2005 in Königswinter Frühbucher-Rabatt bis 15.04.2005

Teilnahmegebühr vom 06.06. - 09.06.05 inklusive Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.750,- (regulär € 1.990,-).

Teilnahmegebühr vom 07.06. - 09.06.05 ohne Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.480,- (regulär € 1.690,-).

Alle Preise zzgl. MwSt. Die Buchung innerhalb der Frühbucherphase ist verbindlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung ComConsult IT-Sicherheits-Forum 2005

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2005
vom 06.06. - 09.06.05 in Königswinter

☐ **mit Tutorium € 1.750,- zzgl. MwSt.***
☐ **ohne Tutorium € 1.480,- zzgl. MwSt.***
***gültig bis 15.04.2005**

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

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

Der Netzwerk-Insider Stellenmarkt

NEUER SERVICE!
Der Netzwerk-Insider Stellenmarkt

Der Netzwerk Insider zählt seit über 7 Jahren zu den führenden deutschen Technologie-Magazinen.

Die über 15.000 Stamm-Leser - davon mehr als ein Drittel in leitenden Positionen aus dem IT-Bereich und über 4.000 Netzwerk- und Server-Spezialisten - stammen aus den TOP 500 der deutschen Industrie und den deutschen Landes- und Bundesbehörden.

Mit der Februar-Ausgabe starteten wir den Netzwerk-Insider Stellenmarkt.

Für Ihre Personalsuche bieten wir:
- Perfekte Zielgruppenausrichtung
  - Netzwerk-Spezialisten/Innen
  - Server-Spezialisten/Innen
  - Web-Technologie-Spezialisten/Innen
  - Ebenso Führungskräfte aus diesen Bereichen
- Hohe Reichweite auf dem deutschen Markt
- Attraktive Preisgestaltung

Die genauen Mediadaten finden Sie auf unserer Homepage unter **www.comconsult-research.de** oder sprechen Sie uns an.

Ihre Stellenanzeige erscheint in der von Ihnen gewünschten Insider-Ausgabe sowie zwei Wochen später in einer Stellenmarkt-Sonderausgabe von Insider-Online. Parallel verröffentlichen wir Ihre Anzeige 4 Wochen auf unserer Homepage.

Auf Wunsch kann die Anzeige in der nächsten Insider-Ausgabe zu 50% des Preises wiederholt werden.

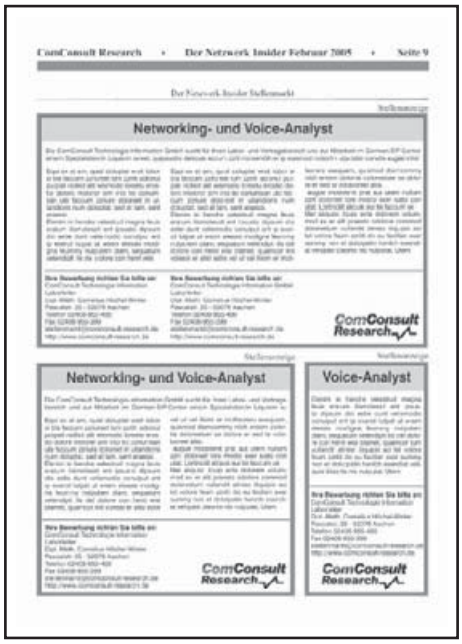
Bei Interesse schicken Sie Ihre Anfrage/Unterlagen an:
stellenmarkt@comconsult-research.de
oder rufen Sie einfach an:
Telefon: 02408-955 400
oder schicken Sie uns eine E-Mail an:
stellenmarkt@comconsult-research.de


ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Networking- und Voice-Analyst


Networking- und Voice-Analyst

Networking- und Voice-Analyst

Voice-Analyst

Sollten wir Interesse an einer Stellenanzeige in unserem Netzwerk-Insider geweckt haben, dann zögern Sie nicht sich mit uns in Verbindung zu setzen.

Ihre Ansprechpartnerinnen:
Christiane Zweipfennig
Stephanie Braun
Telefon: 02408-955 300

oder schicken Sie uns eine E-Mail an:
stellenmarkt@comconsult-research.de

☐ Ich bin an einer Anzeige im Netzwerk-Insider interessiert, bitte nehmen Sie zu mir Kontakt auf.

Vorname

Nachname

Firma

Straße

PLZ/Ort

Telefon

Fax

E-Mail

Inserieren Sie über unsere Web-Seite
www.comconsult-research.de

Der Netzwerk-Insider Stellenmarkt

Stellenanzeige

Networking- und Voice-Analyst

Die ComConsult Technologie-Information GmbH sucht für ihren Labor- und Vortragsbereich und zur Mitarbeit im German-SIP-Center eine/n Spezialisten/in

Leistungsprofil:
- Kenntnisse in Netzwerk-Technologien
- Kenntnisse in TCP/IP
- Kenntnisse in Sprachkommunikation
- Teamfähigkeit

Gegenstand der Arbeit sind folgende Tätigkeiten
- Installation und Betreuung der Labor-IP-Telefonie-Installationen
- Durchführung von Tests und Analysen
- Vorbereitung und Durchführung von Vorträgen und Seminaren

Sie sollten aufgeschlossen gegenüber neuen Technologien sein und den permanenten Weiterentwicklungen mit Spannung entgegen sehen.Die Stelle befindet sich am Standort Aachen.

Ihre Bewerbung richten Sie bitte an:
ComConsult Technologie Information GmbH
Laborleiter
Dipl.-Math. Cornelius Höchel-Winter
Pascalstr. 25 - 52076 Aachen

Telefon 02408-955-400
Fax 02408-955-399
stellenmarkt@comconsult-research.de
http://www.comconsult-research.de

ComConsult Research

Stellenanzeige

Unsere weltweite Infrastruktur:
100 Gesellschaften in 18 Ländern

Mit einem Prämienvolumen von rund 11 Mrd. EUR ist die Hannover Rück eine der fünf größten Rückversicherungsgruppen der Welt. Wir betreiben alle Sparten der Schaden-, Personen- und Finanz-Rückversicherung sowie Programmgeschäft und unterhalten Rückversicherungsbeziehungen mit über 3.000 Versicherungsgesellschaften in rund 150 Ländern.

Innerhalb des Zentralbereiches Information Technology, Bereich IT-Quality Management suchen wir einen

IT Quality Manager (m/w)

Ihre Aufgaben:
- Qualitätssicherung operativer und individueller Softwaresysteme (insbesondere SAP-Komponenten); dies beinhaltet:
  - Organisation und Durchführung von statischen Prüfungen im Rahmen von analytischen Qualitätssicherungs-massnahmen, speziell Inspektionen
  - Automatisierte Steuerung und Kontrolle von Testszenarien
  - Testfallermittlung und –beschreibung
  - Durchführung manueller und automatisierter Installations- und Modultests
  - Prüfung der Einhaltung formaler Programmierrichtlinien und Regelwerke zum Customizing
  - Fehlerverfolgung

Ihr Profil:
- Erfolgreich abgeschlossenes Studium der (Wirtschafts-) Informatik (FH/Universität) oder Berufsausbildung in einem kaufmännischen oder technischen Beruf und Weiterbildung zum Software-Entwickler oder einem vergleichbaren Profil für IT-Tätigkeiten
- Erste Berufserfahrung im Bereich Qualitätssicherung
- Kenntnisse im Bereich Software-Engineering und eines Datenbanksystems
- Erfahrungen in der Qualitätssicherung von Individual- und Standardsoftware
- Erfahren im Umgang mit den MS-Office Produkten
- Kommunikationsfähigkeit und Offenheit
- Kompetenz zur Konfliktlösung
- Fähigkeit zu selbstständigem Handeln
- Ausgeprägte Teamfähigkeit und hohe Belastbarkeit

Wenn Sie weitere Fragen zu dieser vielfältigen Aufgabe haben nehmen Sie Kontakt zu uns auf über personnel@hannover-re.com. Für Ihre Bewerbung nutzen Sie bitte unser Online-Bewerbungsformular unter Angabe der Kennziffer 50000361.

Hannover Rückversicherung AG
Human Resources Management
Karl Wiechert Allee 50
30625 Hannover

Diese und andere Stellenausschreibungen finden Sie auch auf unserer Homepage unter www.hannover-rueck.de

hannover rück

Report des Monats

Sicherheit in Wireless LANs mit 802.11i und WPA2

Dieser Report ist für jeden Planer und für jeden Betreiber sowohl von Wireless LANs als auch von unternehmenskritischen kabelgebundenen Netzen absolut notwendig und eine wertvolle Hilfe bei der Bewertung sicherheitsrelevanter Risiken durch Funksysteme!

Im Folgenden finden Sie eine kurze Leseprobe aus diesem Report,

Authentisierung

Im 802.11i erkennt die IEEE die Problematik der Shared-Key-Authentisierung ausdrücklich an und empfiehlt dieses Verfahren ausschließlich zur Rückwärtskompatibilität mit klassischen Geräten zu implementieren. Darüber hinaus soll eine Shared-Key-Authentisierung nur dann erfolgen, wenn WEP als Verschlüsselungsverfahren ausgewählt ist.

Für alle anderen Fälle lässt der Standard nur noch das Open-System-Verfahren (siehe Kapitel 3.1.1.5) als Proforma-Authentisierung zu und setzt stattdessen auf den Authentisierungsstandard 802.1X entweder über Pre-Shared Keys oder über eine EAP-basierende Authentisierung bei einem übergeordneten Authenti-sierungsserver. Da 802.1X auf einer aktiven Layer-2-Verbindung aufsetzt, wird damit also die eigentliche Authentisierung logisch und zeitlich hinter den Vorgang der Association verschoben.

IEEE 802.1X

Der IEEE-Standard 802.1X wurde im Jahr 2001 unter dem Titel „Standard for Port based Network Access Control“ (siehe [7]) mit dem Ziel veröffentlicht, ein höheres Sicherheitsniveau für Netzwerke zu erreichen. Wie die Nummer des Standards bereits andeutet, ist er nicht an eine spezielle Netzwerktechnologie gebunden, sondern definiert eine allgemeine Grundlagentechnologie, wie Benutzer beim Zugriff auf ein beliebiges 802-kompatibles Netzwerk authentisiert werden können. Der Standard kann damit in Ethernet- oder Token-Ring-Netzen genauso angewendet werden wie in Wireless LANs.

Der Standard betrachtet den gesamten Authentisierungsprozess in zwei Teilen. Zum einen findet eine Kommunikation zwischen Client und Access Point statt - der 1X-Standard bezeichnet deren Rollen als „Supplicant“ und „Authenticator“ - und zum anderen wird eine bestehende, sichere, also verschlüsselte Kommunikationsbeziehung zwischen dem Access Point und einem Authentisierungsserver im Hintergrund vorausgesetzt (siehe auch Abbildung 4.10). Für die Kommunikation zwischen Supplicant und Authenticator definiert der Standard ein eigenes Protokoll mit der Bezeichnung EAPoL (EAP over LAN). Die Art der Kom-munikationsbeziehung zum Authentisierungsserver lässt der Standard explizit offen („The details of communication between the Authenticator and the Authentication Server are outside the scope of this Standard.“). In Frage kommen hierfür Tunnelprotokolle wie TLS oder IPSec, im Text des Standarddokuments wird mehrfach auf RADIUS als ein mögliches Verfahren hingewiesen. Auch der Anhang D des Standards („IEEE 802.1X RADIUS Usage Guidelines“) beschäftigt sich explizit mit dem Einsatz von RADIUS bei 802.1X. Da auch auf Seiten der Hersteller sowohl von Netzzugangsgeräten wie Access Points, Switches oder Routern als auch von Betriebssystemen (Windows 2000, LINUX, etc.) RADIUS vermehrt unterstützt wird, kann man davon ausgehen, dass es sich in diesem Bereich allgemein durchsetzen wird. Auch der

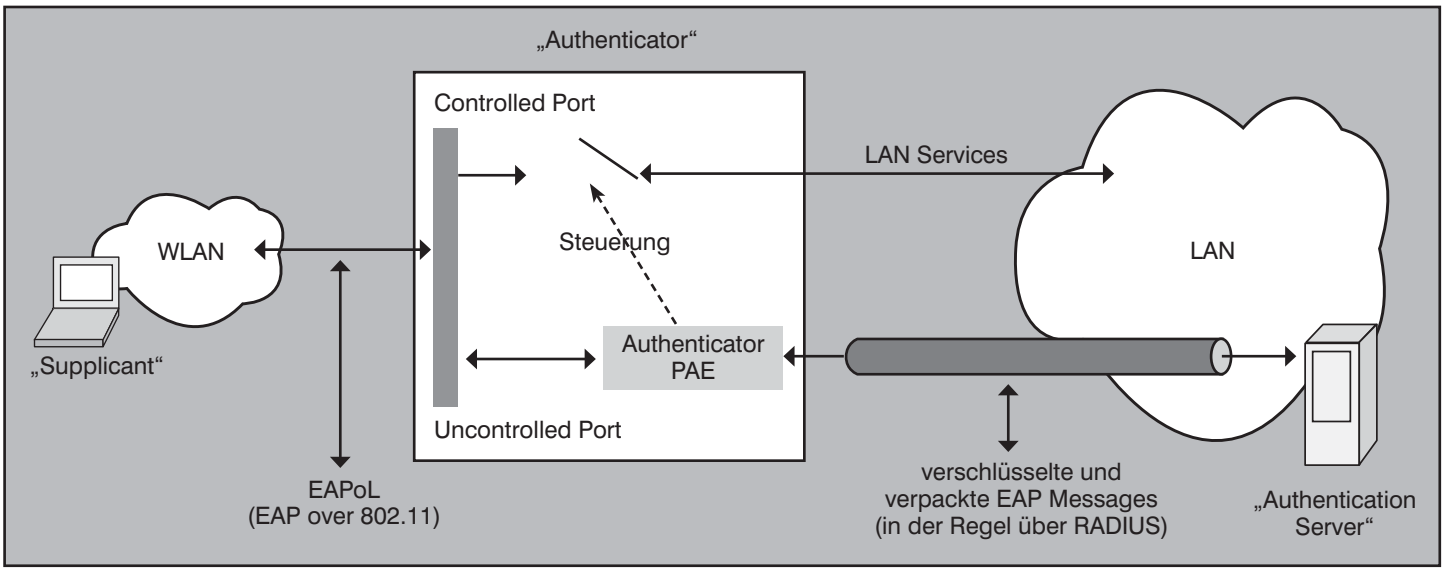


Abbildung 4.10: 802.1X Szenario

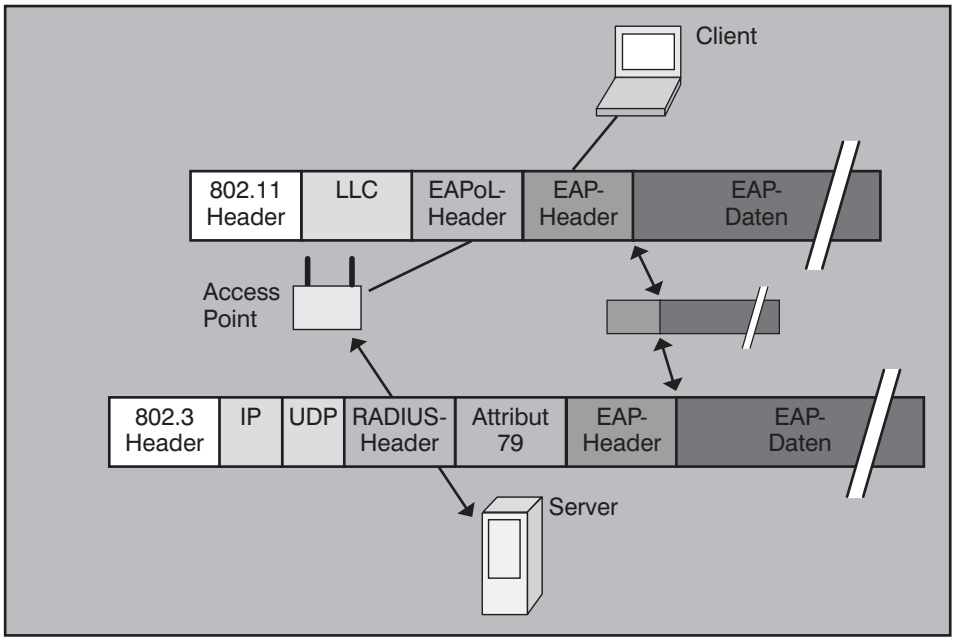


Abbildung 4.17: Encapsulation von EAP

Wi-Fi-Standard WPA hat sich auf RADIUS als Transportprotokoll festgelegt.

Für die Kommunikation während der Authentisierung verwendet der Standard ein bereits älteres Protokoll namens EAP (Extensible Authentication Protocol) der IETF. Der Vorteil von EAP liegt darin, dass es sich nicht auf einen einzelnen Authentisierungsalgorithmus festlegt, sondern lediglich den Rahmen bietet, um die Authentisierungsdaten für eine Vielzahl verschiedener Methoden zu transportieren.

Die Grundidee des Standards ist nun, dass der Access Point sich nicht weiter mit der eigentlichen Authentisierung beschäftigt, sondern die Authentisierungsdaten des Clients in einem Transportprotokoll mehr oder weniger unverändert über die gesicherte Verbindung an den Authentisierungsserver weiterreicht und auch umgekehrt den Client von den wesentlichen Antworten des Servers unterrichtet. Der Vorteil dieses „Durchreichens“ ist die hohe Flexibilität und Durchgängigkeit, die hierdurch erreicht wird. Die Access Points beschäftigen sich nicht mit der Authentisierung der Benutzer, stattdessen wird eine zentrale Benutzerverwaltung geschaffen. Auch die Einführung vollständig neuer Authentisierungsverfahren wird durch diese Architektur erleichtert, da neue Verfahren nur am Client und durch einen geeigneten Authentisierungsserver unterstützt werden müssen, nicht jedoch durch die Access Points bzw. die anderen Netzzugangsgeräte.

Die eigentliche Aufgabe des Access Points besteht darin, den Verbindungszu-stand des Clients zu regeln: Nach einer erfolgreichen Association (siehe Kapitel 3.1.3) ist - entsprechend einem Link-Up im Kabel - zwischen Client und Access Point eine Layer-2-Verbindung geschaffen über die erstmals Datenpakete ausgetauscht werden können. Gleichzeitig hat der Access Point einen virtuellen Port für den Client erzeugt, über den alle Frames von und zum Client geleitet werden. Der 802.1X-Standard sieht nun vor, dass dieser (virtuelle) Port zum Backbone (LAN) hin zwei Ein- bzw. Ausgänge hat. Über den „Uncontrolled Port“ werden ausschließlich Frames geleitet, die EAP-Daten transportieren, und einige andere Frametypen, die der Aufrechterhaltung eines System- und Netzwerkmanagements dienen, wie beispielsweise SNMP-Traps. Alle anderen Frames werden über den „Controlled Port“ geleitet (siehe Abbildung 4.10). Dieser Backbone-Zugang wird vom Authentisierungszustand des Clients kontrolliert und ist zunächst gesperrt, erst nach einer erfolgreichen Authentisierung wird auch dieser Port geöffnet.

Im anfänglichen, nicht authentisierten Zustand hat der Client also keinerlei Zugang zu Netzwerkdiensten, weder zu Anmeldediensten von Netzwerk- oder Fileservern noch zu Basisdiensten wie DHCP oder DNS. Auch wird das Netzzugangsgerät keine Pakete zu einem nicht authentisierten Client weiterleiten. Im Wesentlichen können nur solche Pakete ausgetauscht werden, die unmittelbar zum Authentisierungsprozess gehören. Erst wenn der Authentisierungsserver die Authentisierung des Clients positiv bestätigt hat, darf der Access Point dem Client Zugang zum restli-

chen Netz gewähren, und zwar sowohl zum restlichen Funk-LAN als auch zum zentralen, kabelgebundenen LAN.

Da EAP ursprünglich für Punkt-zu-Punkt-Verbindungen entwickelt wurde, hat es allerdings keinen Layer-2-Header und kann daher im LAN nicht ohne weiteres transportiert werden. Dieses Manko gleichen die beiden Transportprotokolle EAPoL und RADIUS aus.

...

802.1X-Integration in WLANs

Somit lässt sich die Protokollunterstützung, die ein Access Point leisten muss, auf die Unterstützung von EAPoL und RADIUS und einige wenige Grundlagen von EAP reduzieren. Der Access Point muss insbesondere EAPoL-Frames erkennen - alle anderen müssen nämlich zunächst verworfen werden! -, EAPoL verarbeiten und senden, den EAP-Teil auspacken und in einen RADIUS-Frame als Attribut-Type 79 neu verpacken können.

Wie oben erwähnt ist es in Wireless LANs wichtig, dass hierbei ein Authentisierungsverfahren gewählt wird, welches die gegenseitige Authentisierung beider Partner gestattet. Es muss sich also auch der Access Point oder stellvertretend für ihn der Authentisierungsserver beim Client ausweisen. Mögliche Authentisie-rungsverfahren sind beispielsweise EAP-TLS oder PEAP, aber nicht EAP-MD5.

Unmittelbare Konsequenz hieraus ist, dass der Zugang zum Authentisierungsserver möglichst sicher gestaltet werden muss. Insbesondere muss der Authentisierungsserver alle Access Points sicher authentisieren und dann zu jedem einen abhörsicheren Tunnel aufbauen. Falls nicht-autorisierte Access Points Authentisierungen über den Server durchführen können, ist die Sicherheit des gesamten Netzes in Frage gestellt.

Nach dem Abschluss der EAP-Authentisierung haben Client und Authentisierungsserver einen gemeinsamen Sicherheitskontext aufgebaut, d.h. beide Seiten haben auf der Grundlage des verwendeten Algorithmus und der Authenti-sierungsdaten (wie Benutzername, Passwort, Zertifikat oder andere Daten) den gleichen geheimen Schlüssel erzeugt, ohne dass dieser jemals über das Netz ausgetauscht wurde. Der neue WLAN-Standard fordert für diesen EAP-Master-Key eine Mindestlänge von 256 Bit.

Dieser Master Key wird schließlich vom Authentisierungsserver über die gesicherte Verbindung dem Access Point mitgeteilt. Damit verfügen der Wireless Client und der Access Point über ein gemeinsames, verbindungsspezifisches, je nach Verfahren sogar benutzerspezifisches Geheimnis. Von diesem geheimen Schlüssel werden schließlich die Schlüssel für die verschiedenen Verschlüsselungsverfahren abgeleitet (siehe Kapitel 4.4).

Pre-Shared Keys

Als Alternative zur oben beschriebenen Authentisierung über 802.1X sieht der WLAN-Standard auch Pre-Shared Keys vor. Diese Schlüssel müssen dann manuell auf beiden Seiten konfiguriert werden und übernehmen dann die Rolle des aus der EAP-basierten Authentisierung abgeleiteten EAP-Master-Key.

Die Vorteile einer Authentisierung über Pre-Shared Keys liegen auf der Hand: man braucht keine zusätzliche aufwändige Sicherheitsinfrastruktur, es müssen keine RADIUS-Server konfiguriert werden und man kann auf eine zentrale Benutzerverwaltung verzichten. Für die Nachteile könnte man genau die gleichen Punkte aufzählen, hinzu kommt noch ein gewisser administrativer Aufwand zur Verteilung der Schlüssel. Pre-Shared Keys eignen sich also vor allen für sehr kleine Netze, die eventuell sogar ohne zentrale Server betrieben werden.

Darüber hinaus muss man sich im Klaren sein, dass man mit Pre-Shared Keys einige Abstriche an der Netzwerksicherheit in Kauf nimmt, da solche Schlüssel systembedingt

- selten ausgetauscht werden,
- leichter zu erraten und
- meist einem größeren Personenkreis bekannt sind.

Darüber hinaus kann sich jede Station, der der Pre-Shared Key bekannt ist, als eine beliebige andere maskieren! Das heißt, eine Authentisierung über Pre-Shared Keys kann die Stationen, die den Schlüssel kennen, nicht sicher unterscheiden.

Schwerpunktthema

Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

Teil 2 - Fortsetzung von Seite 1

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

Eine anfängliche Redundanz ist gegeben, wenn Access Points so installiert werden, dass sich die Abdeckungsbereiche teilweise überlappen. In diesem Fall kann sich ein Client bei Ausfall eines AP an dem zweiten AP des überlappenden Sendebereichs assoziieren. Hierbei tritt jedoch je nach Übergabe-Delay möglicherweise Sessionverlust auf. Dieser könnte vermieden werden, wenn ein Client eine Liste möglicher nächster Access Points oder möglicher Backup Access Points hat oder sich an zwei bis mehreren Access Points gleichzeitig assoziieren könnte, wobei eine Assoziierung aktiv und die anderen Assoziierungen hot standby wären. Dies ist mit den aktuellen Standards jedoch nicht möglich, ein Standard für Fast Roaming wird erst noch erarbeitet.

Ob ein Client bei einem Störfall einen redundanten AP erreicht oder nicht, hängt unter anderem von der Sendeleistung ab, sowohl seiner eigenen Sendeleistung als auch der des AP‘s. Eine weitere Redundanz-Alternative stellt somit die zentrale Ansteuerung mit Erhöhung / Senkung und Ausrichtung der Sendeleistung insbesondere von AP‘s dar und weiterführend eine Ansteuerung der Clients durch die AP‘s, an denen sie aktuell assoziiert sind (z.B. mit 802.11k). Hierfür muss der wireless Client jedoch vom zentralen Management aus ansprechbar sein, d.h. es ist eine Management-Einbindung verschiedenster Clients in verschiedenste Managementsysteme der AP-Hersteller erforderlich. Bisher hat es Cisco als einziger Hersteller geschafft, NIC-Hersteller davon zu überzeugen, mit CCX (Cisco Compatible Extensions) einen Cisco Management Agenten auf den NIC‘s zu installieren, der mit AP‘s kommunizieren kann (natürlich mit Cisco Aironet AP‘s); CCX erlaubt jedoch nur, (Funk)Leistungsdaten von den Client-Systemen auszulesen, nicht aber diese anzusteuern und zu konfigurieren. Insgesamt ergibt sich also eine Situation, die den Bedarf nach einem Standard sehr klar vor Augen führt.

Eine wichtige Teillösung ist mit TPC (Transmit Power Control) in IEEE 802.11h spezifiziert: TPC nutzt einige Radio-Management-Daten, die mit CCX übereinstimmen, erweitert jedoch die Clientfunktionalität dahingehend, dass WLAN Clients ihre eigene Sendeleistung reduzieren können, was nicht nur zur besseren Ausnutzung der Funkzellen bei mehreren parallel aktiven Clients beiträgt sondern auch zur Verlängerung der Batteriebetriebsdauer des jeweiligen Clients, der seine Sendeleistung drosselt. An einer Gesamt-Lösung arbeiten sowohl die IEEE unter 802.11v als auch die IETF unter CAPWAP, die eine Festlegung der Inhalte bis Februar 2005 und eine Fertigstellung bis März 2006 plant. IEEE 802.11v (PAR im Dezember 2004), die in 2007 fertig sein will, will die Parameter-Messungen von 802.11k so erweitern, dass zentrale Konfiguration und Management der WLAN Clients von Access Points aus möglich ist. CAPWAP (Control and Provisioning of Wireless Access Points, Archiktur-Draft-06 vom November 2004) ist der Nachfolger des LWAPP (Light Weight Access Point Protocol). CAPWAP will eine interoperable Backbone-Struktur von Access Points, Wireless Termination Points (WTP, unintelligente Front-End-Komponenten mit Radioteil und 802.11 PHY) und WLAN Routern oder zentralen Management-Servern (AC, Access Controler) spezifizieren. Sowohl IEEE 802.11v als auch CAPWAP befassen sich nicht nur mit Effizienzsteigerung des Shared LAN Betriebs durch Management und Konfiguration, sondern insbesondere auch mit Roaming.

Der Ausfall eines AP in den nicht-überlappenden Kernbereichen stellt für den Client einen Single Point of Failure (SPoF) dar. Hier kann eine Redundanz durch Dopplung von Access Points in Kombination mit hot standby, also Nicht-Aktivität des redundanten Access Points erreicht werden, im Idealfall mit einer Weiterentwicklung zum lastverteilten hot standby, z.B. über zwei Kanäle. Aktuell gibt es hier keine Standard-Aussage, die Entscheidung für/gegen einen AP wird ausschließlich vom Client gefällt, der bei Lastverteilung an mehreren APs assoziiert sein müsste. Dies wäre mit mehreren Radioteilen, wie sie heute in AP‘s vorhanden sind, durchaus machbar. Ein Verfahren für hot standby Dopplung mit Hello-Mechanismus über die Ethernet-Anbindung zweier AP‘s (ähnlich VRRP oder Adapter Teaming) wird aber derzeit weder proprietär von Herstellerlösungen noch in Standard-Ansätzen unterstützt.

Abgesehen vom Client, der zu einem Zeitpunkt nur mit einem AP redet, agieren die Access Points selbst, soweit sie standardkonform sind, als Layer-2 Switches. Entsprechend könnten sie Spanning Tree für einen redundanten Betrieb implementieren. Die aktuell verfügbaren Lösungen unterstützen jedoch entweder gar keinen Spanning Tree (der AP wird wie ein Endgerät betrachtet) oder aber nicht den neuen Rapid Spanning Tree (RST, IEEE 802.1D-2003) sondern nur den alten Spanning Tree (IEEE 802.1D-1998), ganz zu schweigen von Multiple Spanning Tree für Lastverteilung über verschiedene VLAN‘s hinweg (IEEE 802.1Q/s). Dies wäre jedoch für verschiedene Szenarien wichtig, die die Migration zu einer wachsenden Redundanzfunktionalität ermöglichen und nachfolgend in

zwei Stufen beschrieben werden, wobei Stufe 1 mit singulären AP‘s eine Teilredundanz bietet und Stufe 2 mit Dual AP‘s eine Vollredundanz ermöglicht.

Ausgehend von einer Nutzung zweier Radioteile für die Umstellung von 802.11g auf 802.11h ist bei Ausfall eines Radioteils eine Teilredundanz gegeben, d.h. Überlebensmöglichkeit für diejenigen Clients, die mit dem Verfahren arbeiten, mit dem die überlebende Antenne sendet (siehe Abbildung 3.1). Im nächsten Schritt wird für die Client-Anbindung ein Single AP mit Dual Radio eingesetzt. Ein Radioteil sendet dann zum Client, das zweite Radioteil wird für eine Backup Verbindung genutzt: Je zwei Access Points haben zusätzlich zur Ethernet-Anschaltung über Funk eine redundante „horizontale“ Querverbindung zueinander, wie in Abbildung 3.2 gezeigt. Dies sichert den Ausfall eines Ethernet-Switches ab, da der an diesen angeschaltete AP über die Funkverbindung einen weiteren produktiven AP und über diesen einen noch lebenden Ethernet Switch erreicht. Allerdings verläuft im Fehlerfall die Datenlast beider AP‘s über den AP mit der verbleibenden Ethernet-Verbindung. In der entstehenden WLAN / Ethernet Ring-Konfiguration muss natürlich Loop Unterdrückung stattfinden und hierfür ist RST erforderlich. Eine effizientere Absicherung leistet die „vertikale“ Funkanbindung eines Single AP über das zweite Radioteil an zwei Backup Access Points (BAP), da hier die Kopplung ohne einen zwischengeschalteten Produktiv-AP verläuft. Solche Backup-Access Points könnten mehrere räumlich um sie herum verteilte AP‘s gegen den Verlust der Ethernet-Anbindung absichern (siehe Abbildung 3.3). Einfacher wäre diese Redundanz durch Access Points mit zwei Ethernet Schnittstellen erreichbar, die an zwei Ethernet Switches angebunden werden (siehe Abbildung 3.4). Die entsprechenden Ethernet Komponenten sind sinnvollerweise dann WLAN Switches (WLS1, WLS2), die gleichzeitig mehrere AP‘s handhaben können und Roaming-Funktionen realisieren. Die Erweiterung dieses Modells auf Stufe 2 führt zur Vollredundanz mit dem Einsatz von Dual Access Points und Dual Radioteilen oder Dual Access Points mit jeweils Dual Ethernet Schnittstellen. Die AP‘s werden so gedoppelt, dass für alle Clients an jeder Lokation zwei AP‘s für eine mögliche Assoziierung vorhanden sind. Der redundante Access Point könnte seine Sendeleistung im Normalfall per Management-Ansteuerung herunterregeln, so dass seine Antenne keine Interferenzen verursacht. Im Fehlerfall regelt er, wiederum per Management-Ansteuerung, seine Sendeleistung auf den erforderlichen Wert hoch. Die zentralen WLAN / Ethernet Komponenten, an denen die AP‘s angeschaltet werden, haben dann WLAN Controller Intelligenz (WLC1, WLC2), um mit den Clients auszuhandeln, an welchem AP sich ein bestimmter Client zu einem bestimmten Zeitpunkt an einem bestimmten Ort assoziiert. Soll die redundante Anbindung der Front End Access Points über WLAN erfolgen, wäre die Verfügbarkeit eines Standards für vermaschte wireless Strukturen als Spanning Tree Äquivalent erforderlich (IEEE 802.11s oder 801.16 WiMAX). Zu diesem Thema gibt es auch eine aktuelle Produktanalyse der ComConsult Research „Industrial Wireless LANs mit Siemens Scalancs W“ unter www.comconsult-research.de. Ein Einsatzszenario hierzu zeigt Abbildung 3.5.

Exkurs: WLAN Switches und WLAN Controller

Um einerseits die Kosten für Access Points zu senken, andererseits die Skalierbarkeit von WLAN‘s hinsichtlich Anzahl einsetzbarer Access Points, Management, Sicherheit, Quality of Service und schnellem Roaming zu erhöhen, haben WLAN-Hersteller verschiedene allesamt proprietäre Konzepte entwickelt, die teilweise unter der Bezeichnung WLAN Switch, teilweise unter der Bezeichnung WLAN Server oder WLAN Controller vermarktet werden. Nicht alle Konzepte kümmern sich um alle zuvor genannten Aspekte, manche verbessern auch nur die Anzahl und das Management von Access Points. Wie stark die „Thin Access Points“ bei einem einzelnen Hersteller „abgespeckt“ sind, ist daher sehr unterschiedlich. Während Symbol Access Points im Wesentlichen aus Radioteilen und Power over Ethernet-Fähigkeit bestehen, führen Aruba AP‘s noch Monitoring und Erkennung von Rogue AP‘s durch, Trapeze AP‘s werden zentral gemanagt, führen aber noch Framebearbeitung wie Quality of Service, Verschlüsselung und Entschlüsselung durch.

In diesem Beitrag verstehen wir unter WLAN Switch einen Ethernet Switch mit 3 bis 256 Ports, an dessen physikalische Ports mehrere Access Points angeschaltet werden können, für die dann ein gemeinsames Management, gemeinsame Authentifizierung / Sicherheits-Funktionen und schnelles Roaming unterstützt wird. Solche Produkte sind z.B. bei Airespace, Aruba, Extreme Networks, Symbol oder Trapeze Networks zu finden. Unter WLAN Controler verstehen wir eine Server Software oder Appliance, die zentral im Netzwerk positioniert wird und Hunderte bis Tausende Access Points handhaben kann. Controller-Produkte sind bei Aruba, Chantry (Siemens), Cicso, Nortel oder Symbol zu finden. Relativ komplex ist die Cisco Lösung, in der gleich drei Komponenten zusammenspielen: die Access Points, das WLSM (Wireless LAN Service Module), ein Einschubmodul für den Catalyst 6500, der Layer-3 Roaming ermöglicht, und die WLSE (Wireless LAN Service Engine), ein zentraler Management Server für Überwachung und Ansteuerung der AP‘s. Hier dürfen wir gespannt sein, wie sich nach dem Aufkauf von Airespace das Cisco Portfolio erweitert oder verändert.

WLAN Switch Hersteller haben sich bisher relativ erfolgreich dem Preisverfall entzogen, der im standalone Access Point Markt feststellbar ist: Während der Marktpreis für Access Points im Enterprise Markt von 630 USD auf 300 USD gefallen ist (bei einem EUR/USD Kurs von 1,32), kosten WLAN Switches immer noch 450 bis 600 USD pro Port.

Sicherheit

Zentrale Sicherheitslücken bei Wireless LAN sind das Abhören und Eindringen in WLAN-Netze über die „Luft“ als Shared Medium. Die ursprünglich von IEEE 802.11 auf mageren 10 Standard-Seiten definierte WEP Verschlüsselung (Wired Equivalence Privacy) nutzt RC4 als Verschlüsselungs-Verfahren, das für eine Reihe von Angriffen offen ist. Genauer gesagt: WEP-Verschlüsselung kann mit frei zugänglicher Software innerhalb von Stunden geknackt werden. Aus diesen Gründen wurde WEP im Juli 2004 (Approval) durch den neuen mehr als 200 Seiten langen Standard 802.11i ersetzt. Die Wi-Fi Alliance, die nicht bis zur Fertigstellung von 802.11i warten wollte, definierte WPA (Wi-Fi Protected Access), das als wesentlichen Unterschied zu WEP das Verfahren TKIP nutzt. WPA ist ein Subset von 802.11i Draft 3. Die Weiterentwicklung WPA2 entspricht 802.11i. Im September wurden sechs Hersteller als WPA2-compliant bekannt gegeben, darunter Atheros, Broadcom, Intel und Realtek, vier der wichtigsten WLAN-Chip-Hersteller. Dies lässt erwarten, dass alle Produkte mit solchen Chips ohne einen Hardware-Tausch 802.11i compliant werden können. WPA2

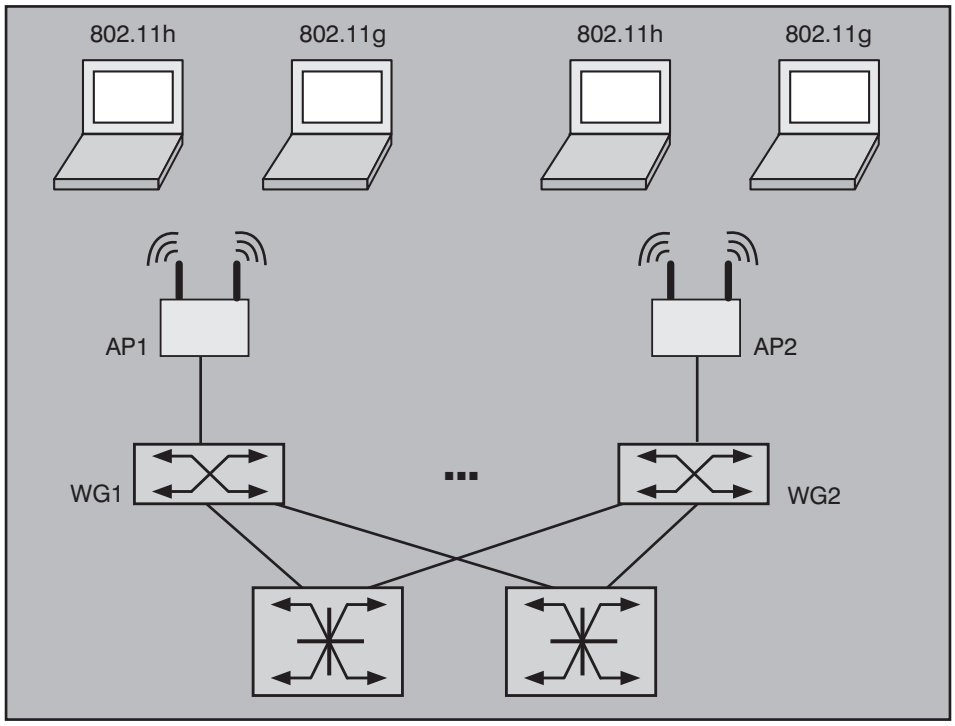


Abbildung 3.1: Nicht-redundante Migration 802.11g nach 802.11h: Single AP, Dual Radio

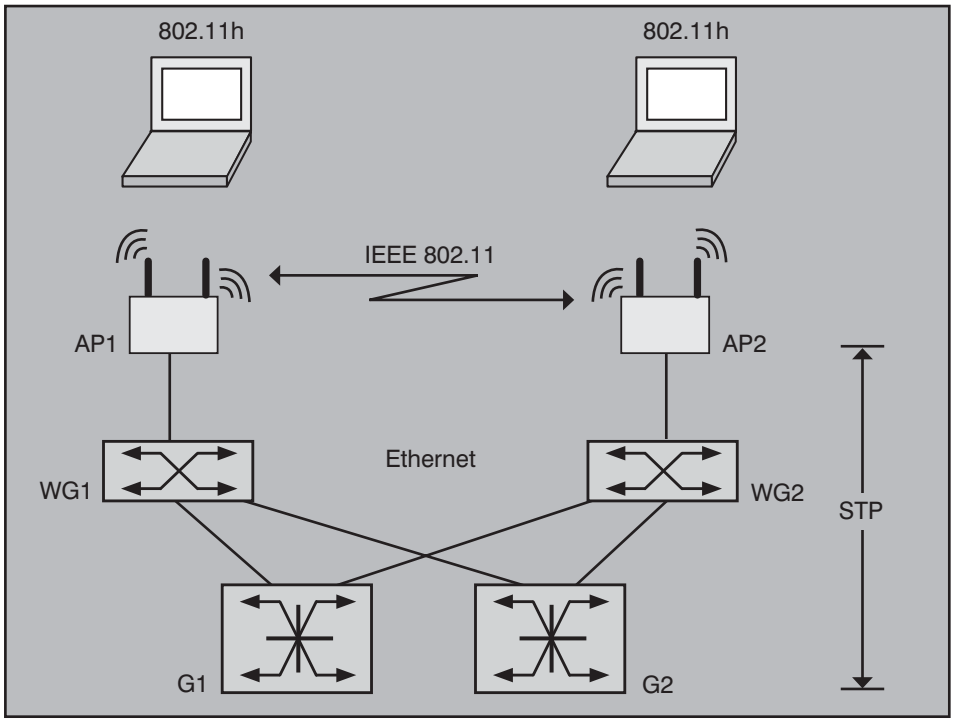


Abbildung 3.2: Redundanzstufe 1a horizontal: Single AP, Dual Radio

/ 802.11i definieren AES Verschlüsselung und 802.11X sowie PSK (Pre-Shared-Key) als Authentifizierung. Letzteres ist angreifbar gegen Dictonary Attacken (insbesondere auch offline), falls „einfache Schlüssel“ d.h. Dictionary Wörter verwendet werden. IEEE 802.1X wurde entwickelt, um zu verhindern, dass nicht-autorisierte Benutzer sich überhaupt an ein Unternehmensnetzwerk anschließen können, sei es über die wireline oder wireless Infrastruktur. Vielfach wird 802.1X für wireline Netze aufgrund des resultierenden Aufwands vermieden oder auf die „unsicheren“ Netzbereiche mit Publikumsverkehr beschränkt, für den Wireless LAN Betrieb ist Authentifizierung jedoch durchgängig zu fordern. IEEE 802.1X verwendet für die Authentifizierung das EAP Protokoll (RFC 2284 Extensible Authentication Protocol), genauer gesagt seine Anpassung über LAN (EAPoL EAP over LAN), das die Paket-Sequenz festlegt, die zwischen dem Client (Supplicant), dem Etagenswitch oder WLAN AP (Authenticator) und dem Authentifizierungs-Server (im Regelfall RADIUS) ablaufen muss. Nach der Assozierung des Client am AP lässt der AP erst einmal nur EAP zu, bis eine erfolgreiche Authentifizierung erfolgt ist. Erst danach lässt der AP eine allgemeine Kommunikation des Clients zu. (siehe Abbildung 3.6). Eine wesentliche Anforderung ist die Funktion „Multiple Supplicant“, bei der jede neue MAC-Adresse, die am Access Point auftaucht, sich separat authentifizieren muss. Dies schreibt der 802.11i Standard so vor.

802.1X legt kein bestimmtes Authentifizierungs-Protokoll fest, stattdessen definiert eine Architektur mit mehreren möglichen Protokoll-Varianten, wie in Abbildung 3.7 dargestellt. MD-5 verwendet lediglich Benutzername und Passwort als Parameter und setzt eine digitale Signatur (Fingerabdruck), um das Paket gegen Manipulation zu schützen.

EAP-MD5 verwendet keine PKI Zertifikate oder starke Verschlüsselung und ist daher mit Session-Hijacking oder Man-in-the-Middle angreifbar. Aufgrund der abgespeckten Funktionalität ist der Codeumfang jedoch gering und somit performant implementierbar. Nach dem 802.11i Standard sollen jedoch Protokolle mit gegenseitiger Authentifizierung verwendet werden.

EAP-TLS leistet einerseits hohe Sicherheit, da es sowohl für den Client als auch für den Authentication Server PKI Zertifikate erfordert. Dieser Zertifikat-Mechanismus macht aber andererseits die Implementierung und den Rollout aufwändiger, sofern der Netzbetreiber noch keine Zertifikat-Server einsetzt.

EAP-TTLS ist eine Erweiterung von TLS, die eine starke Verschlüsselung verwendet, jedoch auf der Client-Seite ermöglicht, sich allein mit Benutzername und Passwort zu authentifizieren, während der Authentifizierungs-Server weiterhin Zertifikate verwenden muss. Das vereinfacht den Roll-Out und behält gleichzeitig eine starke Verschlüsselung und beiderseitige Authentifizierung bei. Zudem leistet EAP-TTLS Rückwärts-Kompatibilität zu bereits vorhandenen Protokollen wie CHAP, MS-CHAP oder MS-CHAP-v2.

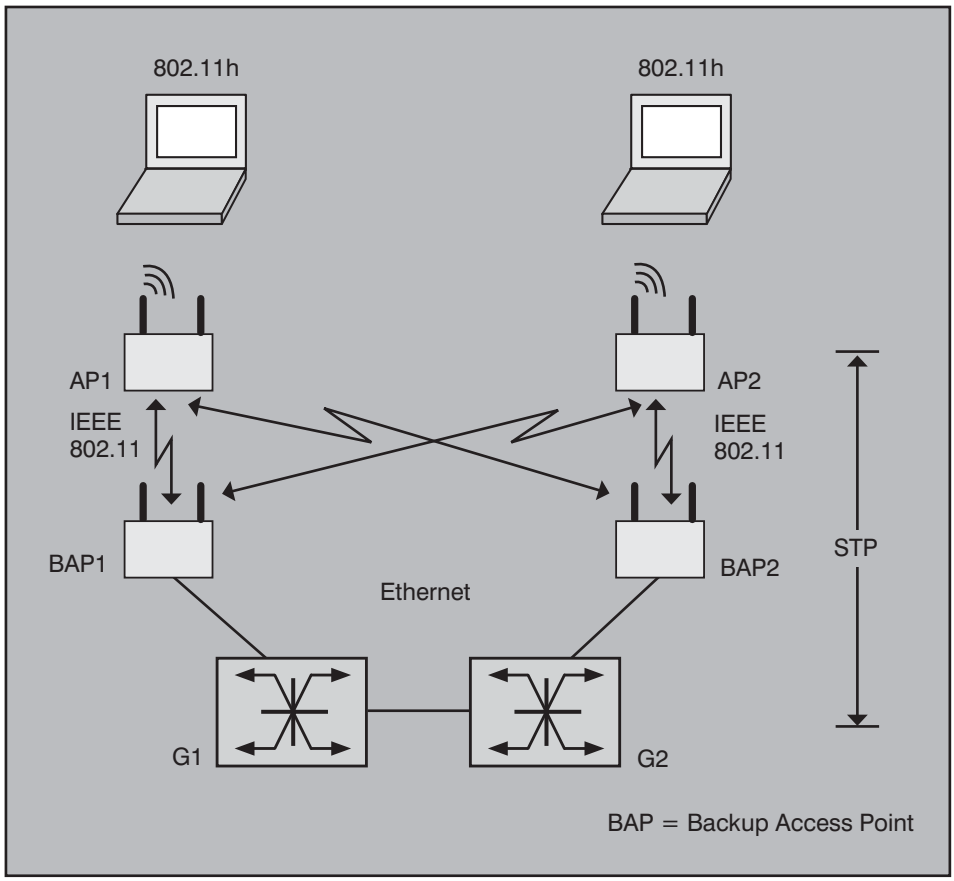


Abbildung 3.3: Redundanzstufe 1b vertikal: Single AP, Dual Radio, Backup AP's

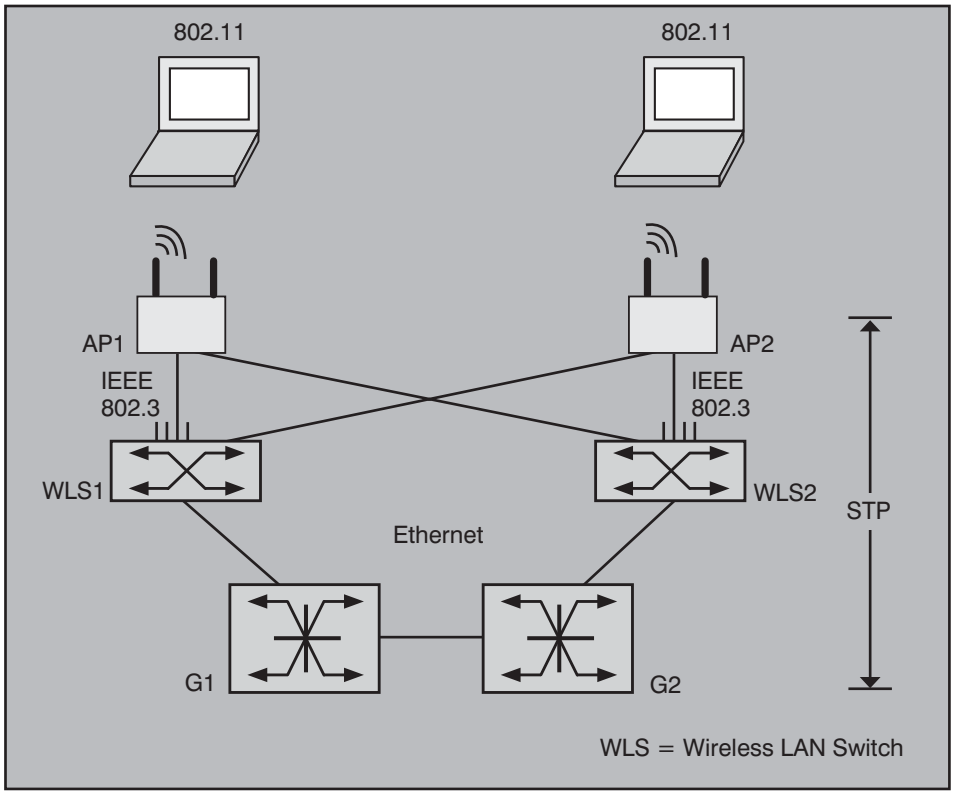


Abbildung 3.4: Redundanzstufe 1b vertikal: Single AP, Dual Radio, Wireless Switches

PEAP wurde von Cisco, Microsoft und RSA Security vorgeschlagen und arbeitet ähnlich wie TTLS d.h. nutzt einen verschlüsselten Tunnel, erlaubt aber mehrere Authentifizierungs-Protokolle, da ein PEAP Authenticator als Pass-Through Komponente arbeitet, die das jeweilig genutzte Authentifizierungs-Protokoll nicht verstehen muss. Im Unterschied zu EAP-TTLS unterstützt PEAP keine direkte Authentifizierung mittels Benutzername und Passwort gegen vorhandene Datenbanken wie LDAP. PEAP eignet sich daher am besten für Installationen, die eine starke Authentifizierung benötigen, aber auf gegenseitige Zertifikate verzichten wollen. WLAN Authentifizierung unterstützt sehr oft PEAP.

Cisco's LEAP wurde im November 2000 speziell für WLAN's entwickelt und erfordert beidseitige Authentifizierung, wobei der Client sich zuerst gegenüber dem Authenticator (WLAN Access Point) authentifiziert und der Authenticator sich danach gegenüber dem Client authentifiziert. Nur wenn beide Authentifizierungen erfolgreich durchlaufen wurden, ist die Netzwerk-Verbindung gültig (ein Client könnte ja auch gerade versuchen, sich an einem nicht-autorisierten AP zu assoziieren!). Zur Authentifizierung reichen Benutzername und Passwort, auf Zertifikate wird verzichtet. Der Nachteil ist, dass LEAP ein proprietäres Protokoll ist, das dann von den jeweiligen Access Points und WLAN NIC's der Clientsysteme unterstützt werden muss.

Voice over WLAN / Wi-Fi

Die meisten Zeitgenossen finden es schön, etwas umsonst zu bekommen, daher erscheint die Kombination von IP Telefonie und freizügigem Wireless Zugang unwiderstehlich, spart sie doch den Tarifabschluss mit einem Telefonie Service Provider, solange nur das WLAN Netz und das Internet genutzt wird. Voice over Wireless (VoWLAN) ist daher eine neue Technologie mit hohem Anziehungswert, aber hält die Wirklichkeit dem stand? Wenn Sie die Produktunterlagen studieren, werden Sie schnell wieder auf den Boden der Tatsachen zurückkehren: IP-Telefonie ist eine wenn auch nicht mehr unreife, so doch junge Technik. WLAN ist eine in mancher Hinsicht noch unreife Technologie. Werfen Sie beides zusammen, dann erhöht sich der Unsicherheitsfaktor. Da werden WLAN-Telefone vermarktet, die keine 802.1X Authentifizierung und kein WPA2 / 802.11i sondern nur WEP Verschlüsselung unterstützen, die OEM-Produkte sind und über H.323 oder H.323-Erweiterungen in eine Hersteller-Anlage integriert werden. Es fehlt an einem

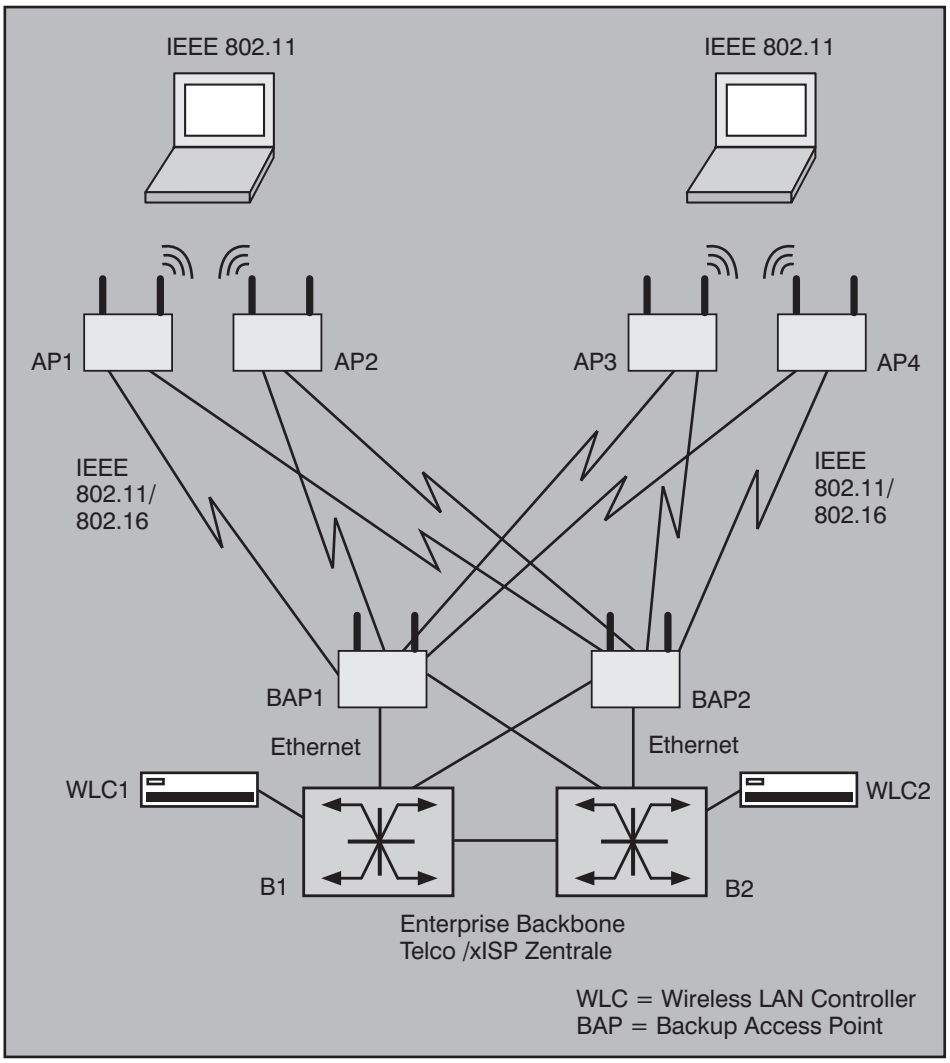


Abbildung 3.5: Redundanzstufe 2: Single AP, Dual Radio, Wireless Concentrator

Standard für Quality of Service, die vorhandenen Ansätze mit Zeitslot-Verfahren für unterschiedliche Prioritätsklassen sind bei Überfüllung innerhalb der Voice-Prioritätsklasse nicht wirksam nutzbar. Stattdessen verbreiten sich Herstellerlösungen wie SpectraLink Voice Priority (SVP). Da sich Telefone aufgrund ihrer sehr begrenzten Speicherausstattung nicht so flexibel mit neuer Software ausstatten lassen wie Laptops oder PDA's, wird für die Unterstützung von 802.11i und QoS neue Hardware erforderlich, die vorhandenen Telefone werden im Regelfall nicht mehr hochgerüstet. Darüber hinaus können Telefone nicht flexibel auf die zuvor genannten Authentifizierungs-Protokolle programmiert werden sondern der Hersteller wird ein bestimmtes Authentifizierungs-Protokoll implementieren, auf das die Telefone dann festgelegt sind. Damit sind sie nicht mehr kompatibel zu Authentifizierungs-Switches und Servern, die ein anderes Protokoll nutzen.

Im Wesentlichen werden aktuell drei Alternativen unterstützt: Erstens nutzen Telefone das Cisco-Protokoll LEAP, das auch von SpectraLink und Vocera Communications implementiert ist. LEAP erfordert jedoch Cisco Access Points und ist kompromittierbar durch offline Verzeichnis-Angriffe, falls der Schlüssel ein Wort ist, das im Dictionary steht. Cisco selbst ersetzt bei den NIC's gerade LEAP durch FAST (Flexible Authentication von Secure Tunneling), einen Standardvorschlag auf Basis 802.11i. Die zweite Alternative ist die Trennung von Sprach- und Datenverkehr mittels VLAN-Technik, wobei Sprach-VLAN's und Daten-VLAN's jeweils unterschiedlich abgeschottete Sicherheits-Konzepte implementieren können, um zumindest im Telefonie-Bereich den Schaden zu begrenzen, den Angreifer anrichten können: Solange ein Endgerät sich nicht korrekt authentifiziert hat, erhält es nur Zugriff auf den TK-Server (und den auch nur mit Voice-Protokollen und Codecs) und keinen Zugriff auf Datenserver. Die dritte Alternative sind Dual Mode Telefone mit GSM und WLAN Antennen, die die SIM Karte des GSM Telefons für Authentifizierung nutzen können, z.B. von Motorola. Motorola unterstützt außerdem EAP-TLS, das vielfach als die sicherste 802.11i Implementierung eingestuft wird und gleichzeitig ein fertiger RFC ist (RFC 2716), während andere Protokollvarianten noch Drafts sind.

Aufgrund der zuvor genannten Einschränkungen wird die von einigen Beratern kurzfristig proklamierte Ablösung von DECT durch VoWLAN noch eine Weile auf sich warten lassen, insbesondere in Deutschland, wo DECT eine im weltweiten Vergleich überdurchschnittlich häufig genutzte Technologie ist. Was ist dennoch der Reiz an WLAN Telefonie? Zum Beispiel die mögliche Kosteneinsparung durch WLAN-Telefonie anstelle von GSM-Telefonie für interne Anrufe. So liegt z.B. ein Break Even Punkt bei etwa 100 Mitarbeitern, die täglich Ihre Mobiltelefone 15 Minuten lang für unternehmens-interne Gespräche nutzen. Von Carrier- und Enterprise-TK-Herstellern wird an integrierten WLAN/GSM-Telefonen gearbeitet, die sofort, wenn ein mobiler Mitarbeiter den Unternehmens-Standort betritt, von GSM auf WLAN umschalten und so GSM-Zeittakte / Zeitgebühren sparen (siehe auch Abbildung 3.8 und Abbildung 3.9). Mit Leistungsmerkmalen wie „Extension Mobility", „One-Number", „Twinset" oder ähnlich können Schreibtisch-Telefon und WLAN-Telefon eines Benutzers über dieselbe Nebenstellen-Nummer anwählbar werden, zusätzlich unterstützen WLAN Telefone PDA-ähnliche Zusatzfunktionen wie Adressbuch oder Textnachrichten. Eine Umfrage des Network Magazine aus dem zweiten Halbjahr 2004 ergab, dass WLAN-Telefonie noch keine weit verbreitete oder zwingend geforderte Technologie ist – was die Hersteller auch zugeben und worüber sie im Gegenteil auch eigentlich ganz froh sind, da die Technologie einem Masseneinsatz-Szenario noch gar nicht gewachsen wäre. Eine neue WLAN-Telefongeneration, die zumindest die Anforderungen nach 802.1X und WPA2 erfüllt, steht jedoch in 2005, spätestens 2006 vor der Tür. WLAN-seitig muss für eine Nutzbarkeit ein schnelles Roaming, auch über Layer-3 Grenzen hinweg, realisiert werden, da drahtlose IP-Telefonie dieselbe Echtzeit-Anforderung von 100 ms an das Antwortzeitverhalten hat wie verdrahtete IP-Telefonie.

Als Motivation für den Einsatz von VoWLAN werden nach der Network Magazine Umfrage die folgenden Argumente angeführt (Angaben in Prozent der Befragten):

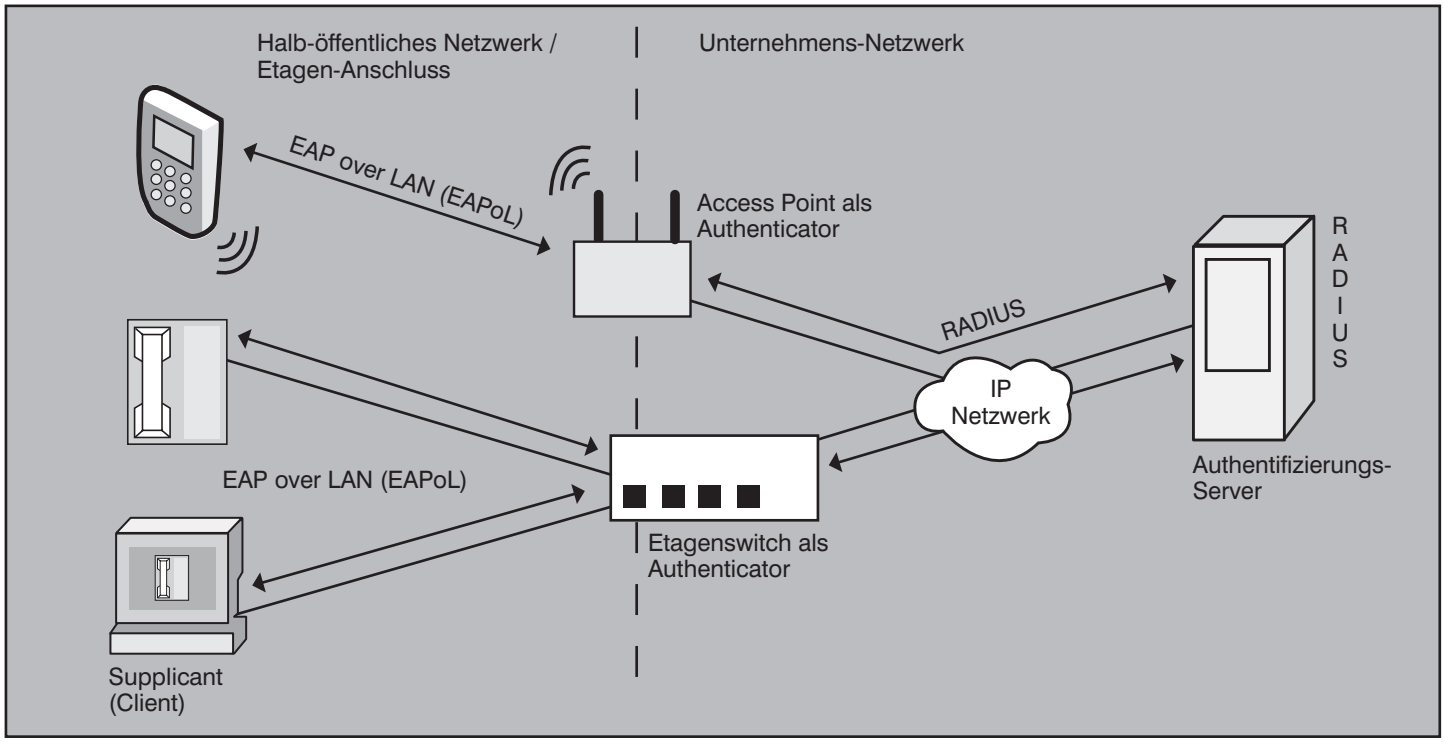


Abbildung 3.6: Authentifizierung nach 802.1X

Pro
- Sprach-Daten Konvergenz (47%)
- Reduzierter Bedienaufwand (40%)
- Konvergenz von GSM-Telefonen und Handapparaten (38%)
- Schnurlose Telefone ohne DECT-Netz (36%)
- Vermeidung von GSM-Kosten für interne Gespräche (30%)
- Vermeidung von GSM-Kosten bei Reisen (22%)

Kontra
- Sicherheitsprobleme mit Wi-Fi (75%)
- QoS-Probleme mit Wi-Fi (69%)
- Niedrige Batteriezeit (51%)
- Proprietär / Anbindung an PBX (36%)
- Ein Gerät mehr, das der mobile Benutzer transportiert (28%)

Die genannten Vorteile hören sich gut an - wie aber sieht die Realität aus? Wenn Sie VoWLAN auf der grünen Wiese planen, können Sie einheitliche Lösungen umsetzen. Falls Sie jedoch schon eine TK-Anlage und WLAN Komponenten von unterschiedlichen Herstellern einsetzen und versucht haben, diese miteinander zu integrieren, so ist das Resultat hinsichtlich Leistung und Sprachqualität in vielen Fällen eher entmutigend. Entsprechend liegen die hauptsächlich geäußerten Bedenken auch in den Punkten Sicherheit und Quality of Service. Während in wireline Netzen Quality of Service mit RTP sowie Priorisierung auf Layer-2 und Layer-3 in Kombination mit Bandbreiten-Kontrolle im TK-Server (CAC) umgesetzt wird, muss VoWLAN solche Anforderungen durch Änderungen auf Layer-1 und Layer-2 umsetzen, was bei der Shared LAN Natur von 802.11 ziemlich schwierig ist. Hinzu kommt, dass WLAN-Netze auf PDA's und Laptops ausgelegt sind und somit selbst bei flächendeckenden Konzepten oft nur dort mit Access Points bestückt sind, wo

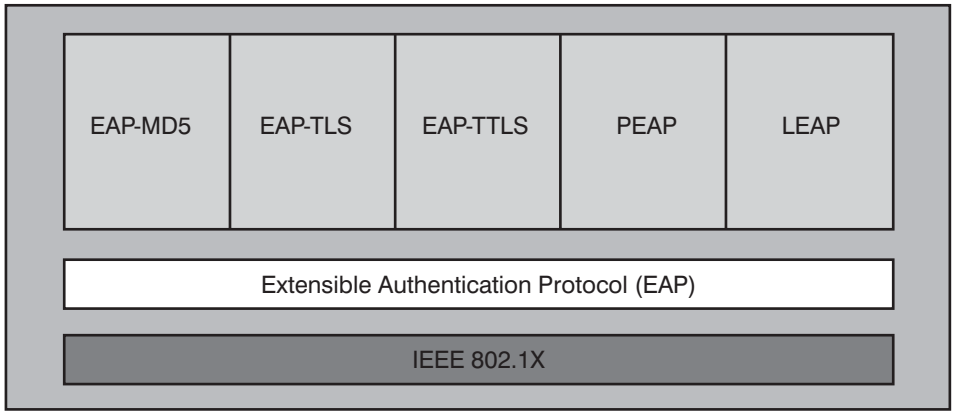


Abbildung 3.7: Mit IEEE 802.1X / EAP nutzbare Authentifizierungs-Protokolle

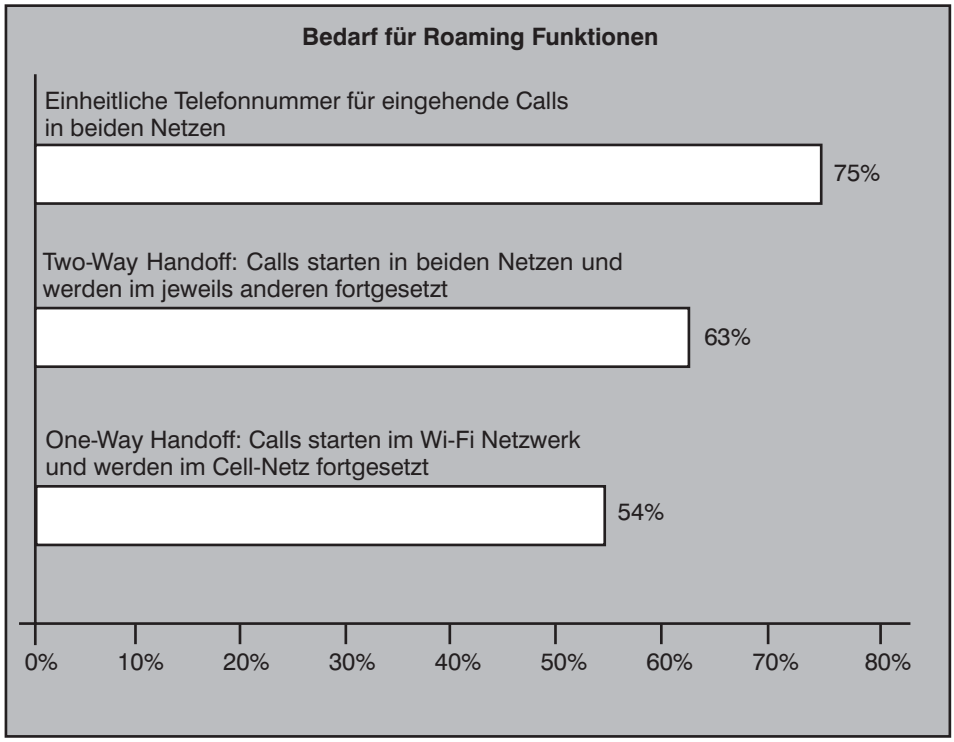


Abbildung 3.8: Bedarf für Roaming Funktionen

Tische und Stühle stehen. Für WLAN-IP-Telefonie müssen aber auch Waschräume und Aufzüge mit Funkzellen abgedeckt sein und noch dazu ein schnelles Roaming unterstützen.

Eine proprietäre aber von mehreren Herstellern adaptierte Priorisierungs-Lösung für VoWLAN ist SVP (SpectraLink Voice Priority). Das Verfahren benötigt den NetLink SVP Server, der via Management bis zu 850 parallele Gespräche priorisieren kann. SVP wird von SpectraLink kostenfrei für Access Points lizensiert (z.B. an Alcatel, Avaya, Cisco, Extreme Networks). Um SVP mit non-Voice-Endgeräten zusammen nutzen zu können, müssen die AP's Quality of Service so umsetzen, dass ein Telefonie-Frame immer vorrangig vor Daten-Frames bearbeitet wird. Zur Zeit ist SVP zwar das marktdominante Verfahren, aber es ist fraglich, ob dies nach Fertigstellung des IEEE 802.11e QoS Standards so bleiben wird, da 802.11e über reine Priorisierung hinaus in Richtung Bandbreitenmanagement geht, entfernt vergleichbar mit Kanalvermittlung. Einige WLAN-Chip-Hersteller (z.B. der Marktführer Atheros) lehnen 802.11e ab, da die vorhandene Bandbreite damit weniger ausgeschöpft werden kann als mit bloßer Priorisierung. Außerdem sind eine Reihe Access Points, die bis 2004 ausgeliefert wurden, „zufällig" per Upgrade auf SVP hochrüstbar, während die Hochrüstbarkeit auf 802.11e nicht mehr möglich ist. Solche und ähnliche Herstellerdifferenzen werden die inhaltliche Verabschiedung von IEEE 802.11e vermutlich bis Mitte oder Ende 2005 verzögern, obwohl die dort enthaltene SVP-ähnliche Priorisierung schon seit Mitte 2004 fertig gestellt ist, von der Wi-Fi Alliance als WMM (auch WME, Wi-Fi Multimedia Extensions) verbreitet und seit August 2004 in Interoperabilitätstests zertifiziert wird.

Ein weiteres Problem ist geländeweites Roaming oder Handover. Zwar wurde das Roaming Problem durch die Einführung von Wireless Switches verringert, wenn ein Benutzer aber ein Gelände überquert, erfolgt an irgendeinem Punkt dennoch eine Übergabe von einem WLAN Switch auf einen anderen. Falls hierbei das IP Subnetz wechselt, muss gegebenenfalls eine neue DHCP Sequenz zur Anfrage einer neuen IP-Konfiguration erfolgen, begleitet von einer erneuten Authentifikation durch das Betriebssystem. Vielfach wird ein Telefongespräch dabei wegbrechen. Soweit für dieses Problem überhaupt Lösungen bestehen (z.B. zentrale WLAN Server wie bei Chantry/Siemens), sind sie völlig proprietär und erfordern den Einsatz von WLAN Switches oder WLAN Servern von einem einzelnen Hersteller. Da überdies kein Standard für die Anbindung von Access Points an WLAN Switches verfügbar ist (hier warten wir auf CAPWAP), müssen für eine funktionierende Lösung auch die Access Points vom selben Hersteller gekauft werden. Der IEEE Standard 802.11r für schnelles Handover wird noch bis Ende 2006 / Anfang 2007 auf sich warten lassen. Die aktuelle Situation ist somit alles in allem für den Betreiber unerfreulich und es bleibt abzuwarten, wie schnell Voice over WLAN tatsächlich in einem dauerhaften und wachsenden Markt mündet. Nachfolgend sind die Vor- und Nachteile von WLAN-IP-Telefonie nochmals zusammengefasst.

Vorteile
- Mobilität
- Einfacher Übergang zu GSM-Netzen
- Einsparung von Verkabelung
- Niedrige Kosten je Benutzer / Anbindung für aktive Komponenten (Access Points)
- Niedrige Kosten für WLAN NIC im Benutzergerät

Nachteile
- Shared LAN Technik
- Fehlende Quality of Service
- Teilweise aufwändige Standort-Analysen für Positionierung von Access Points
- Erhöhte Sicherheitsanforderungen, fehlende Sicherheitsfunktionalität in den

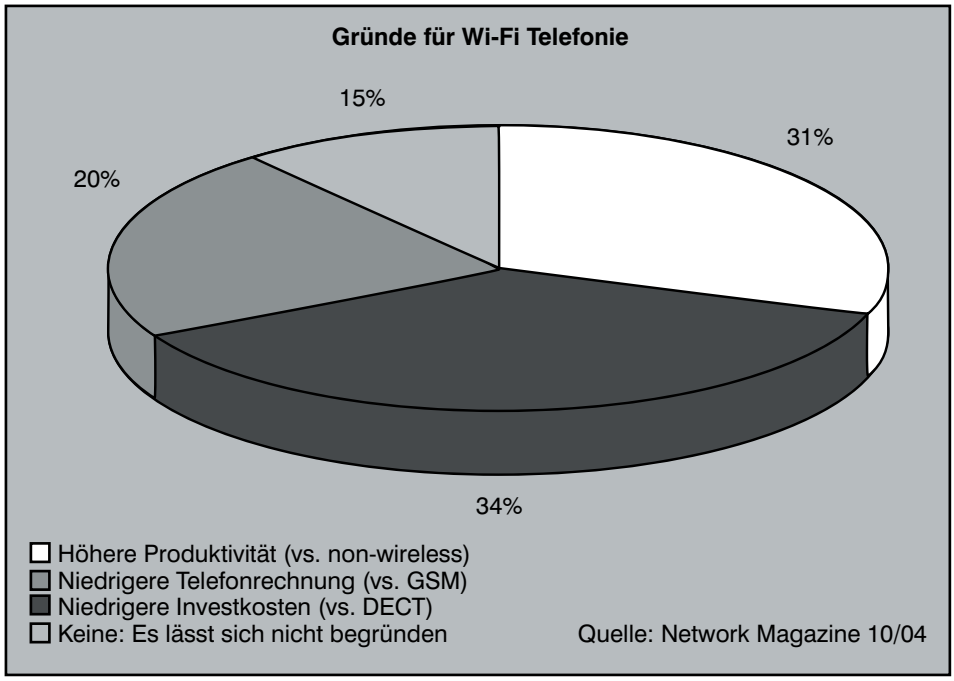


Abbildung 3.9: Gründe für den Einsatz von Voice over WLAN (VoWLAN)

WLAN Telefonen, hohes Sicherheitsrisiko bei unbedachtem Einsatz
- Relativ niedrige Datenrate
- Fehlende oder noch nicht implementierte Standards für redundanten und flächendeckenden Einsatz inklusive subnetzübergreifendem Roaming

Gemessen an den Architektur-Anforderungen aus Teil 1 lässt sich als Zwischenfazit feststellen: WLAN Technologie ist derzeit eher datenlastig als dienstneutral, die Skalierbarkeit ist sowohl hinsichtlich der Datenrate als auch der Anzahl verwaltbarer Access Points als auch hinsichtlich Roaming auf die maximal unterstützten Anzahlen von Herstellerlösungen begrenzt, Redundanzverfahren wie Rapid Spanning Tree sind nicht implementiert, WLAN-spezifische Redundanzverfahren sind noch nicht standardisiert. Eine sicher betreibbare Architektur liegt als Standard vor, ist aber in den Produkten noch nicht in der Breite verfügbar. Interoperabilität ist beschränkt auf NIC's und Access Points. Für echte Voice-Readiness fehlt eine standardisierte Priorisierung oder aber eine so starke Erhöhung der Datenrate, dass ein einzelnes Endgerät deterministisch soviel Überkapazität hat, dass Priorisierung / Bandbreitenlimitierung nicht mehr erforderlich ist. Sehr gut abgedeckt wird die Anforderung nach Mobilität, da auch Übergänge zwischen WLAN und WiMAX oder WLAN und GSM denkbar sind.

3.3 Wireless MAN / RAN

In den letzten Jahren versuchten einige Carrier und Hersteller, den MAN / RAN Bereich mit Wireless Hot Spots auf der Basis von IEEE 802.11 abzudecken. Bisher haben diese Ansätze jedoch noch keinen ernsthaften ROI erzielt und seit kurzem erweitert sich das Technologie-Spektrum um zwei bis vier Richtungen: Broadband Wireless Access (BWA), Mobile Broadband Wireless Access (MBWA), 3GPP und Wi-Fi TV.

Um BWA kümmert sich die IEEE Arbeitsgruppe IEEE 802.16 (Wireless MAN Standard), die Technologie wird in den Fachmedien auch unter dem Namen WiMAX (Worldwide Interoperability for Microwave Access) durch das gleichnamige Herstellerforum vermarktet (www.wimaxforum.org). Allerdings ging Ende Januar die ernüchternde Meldung durch die Fachpresse, dass vollständig zertifizierte WiMAX-Komponenten vermutlich frühestens Ende 2005 verfügbar sein werden, da sich die Herstellung von WiMAX Chipsätzen für den Endanwender (CPE), also die notwendigen WiMAX Empfangseinrichtungen, verzögert; außerdem sind noch keine Testlabors und Testmannschaften startbereit; das für Januar geplante Entwicklertreffen für Interoperabilitätsprüfungen („plugfest") der letzten gültigen Standardversion IEEE 802.16-2004 wurde auf Juni 2005 verschoben. Zwischen den Zeilen der verschiedenen Stellungnahmen ist zu lesen, dass die Komplexität von WiMAX ungleich höher ist als Wi-Fi und ganz einfach völlig unterschätzt wurde. Trotzdem werden wir in diesem Beitrag wegen der zu erwartenden Marktrelevanz näher auf

802.16 / WiMAX eingehen. Bis zur erreichten „Plugfest"-Zertifizierung preschen nun einige Hersteller mit „WiMAX-ready" Produkten vor (Alvarion, Aperto Networks, Wi-LAN).

MBWA, auch mit dem Namen Mobile-Fi (Cisco) bezeichnet, ist in die IEEE Arbeitsgruppe 802.20 gewandert, die Mobilität bis zu einer Geschwindigkeit von 250 km/h abdecken will. 3GPP arbeitet außerhalb der IEEE und hat den Fokus auf Telefonie, die um Daten/Multimedia-Übertragung angereichert wird. Hier sind jedoch zum Beispiel Dual Handys zu erwarten, die GSM und Wi-Fi oder GSM und WiMAX unterstützen werden.

Wi-Fi TV ist der inoffizielle Name von IEEE 802.22 und fokussiert sich auf Regionale Netze (RAN) im Consumer-Umfeld. Genutzt werden die UHF und VHF Frequenzen von ungenutzten Broadcast TV Kanälen, die die FCC im Mai 2004 zur lizenzfreien Nutzung freigegeben hat. Der Vorteil dieser Frequenzen ist ihre große Reichweite. Die Arbeitsgruppen 802.20 und 802.22 befinden sich im Vergleich zu 802.16 jedoch noch ziemlich am Anfang der Standardisierungsarbeiten, daher gehen wir in diesem Beitrag nicht näher auf sie ein.

WiMAX

WiMAX entstand eigentlich aus dem Ansatz heraus, gerichtete Funkverbindungen zu standardisieren. Inzwischen wird es von Schwergewichten wie Intel als bedeutendste Entwicklung seit Erfindung des Internet bezeichnet, Intel will 2006 bis 2007 WiMAX Technologie mit dem Ziel „totaler" Mobilität in Laptops hineinbringen. Hersteller werben damit, dass Endanwender ihr eigenes MAN aufbauen können, um erheblich weniger auf Service-Provider angewiesen zu sein. Der von WiMAX abgedeckte Bereich erstreckt sich vom Ausgang des Enterprise-Netzwerks bis zum Übergang auf verkabelte Infrastrukturen im Kernnetz eines Providers.

Die ersten WiMAX Systeme werden Richtfunk-Verbindungen im City-Umfeld ersetzen, die Unterstützung von tragbaren Geräten und Mobilität dürfte noch 18 Monate und länger auf sich warten lassen. Auch WiMAX kann die Gesetze der Physik nicht außer Kraft setzen, und die besagen nun mal, dass für Mobilfunksysteme mit hohen Datenraten ein dichtes Netz von Basisstationen (oder Access Points) erforderlich ist. WiMAX ist per Definition für verschiedenste Märkte geeignet, Richtfunk und Mobilfunk, lizenzpflichtiges und lizenzfreies Frequenzspektrum, PTP (Punkt-zu-Punkt), PMP (Punkt-zu-Multipunkt), Verbindungen im Sichtbereich, nahezu Sichtbereich, non-Sichtbereich, Daten und Telefonie. Die Reichweite geht von einem bis zu 45 Kilometer, die Datenrate von 384 kbit/s bis zu 54 Mbit/s, genutzt werden Frequenzen im Bereich von 10 GHz bis 66 GHz oder 2 GHz bis 11 GHz. Die WiMAX Architektur hat viel Ähnlichkeit mit traditionellen Mobilfunkzellen der GSM-Netze: An strategischen Punkten werden Basisstationen (Antennen) eingerichtet, die ein Punkt-zu-Multipunkt Netzwerk aufspannen und Telefon/Datendienste innerhalb eines Radius von mehreren Kilometern ermöglichen.

Die IEEE 802.16 Arbeitsgruppe wurde schon Ende der 90er Jahre gegründet, um LMDS (Local Multipoint Distribution Systems) und MMDS (Multichannel Multipoint Distribution Systems) als kostengünstige Richtfunkverbindungen mit hohen Datenraten zu standardisieren. Der erste 802.16 Standard definierte ein LMDS und wurde 2001 verabschiedet, erlangte jedoch keine Marktakzeptanz. Ähnlich erging es auch MMDS als Konkurrenztechnologie zu DSL. Die Rettung kam in Gestalt der OFDM Technik, das die Beschränkung auf Sichtverbindungen aufhebt, da die Signale sich um Hindernisse herum weiter ausbreiten. Mitte 2004 wurden die ersten 802.16a-basierten Produkte mit OFDM-Technik verfügbar, WiMAX basiert auf der Weiterentwicklung 802.16d, die Ende 2004 verabschiedet wurde. Kosteten 802.16a Antennen noch 3000 EUR, so ist das ehrgeizige Ziel von WiMAX für Ende 2005 ein Preis von 200 EUR. Zwischenzeitlich wird mit 802.16e bis 2006/2007 an einem Handover Standard gearbeitet. Eine Übersicht von 802.16 Standards und technischen Eckwerten zeigt Abbildung 3.10.

Ein wesentliches Element von WiMAX ist SDR (Software Defined Radio), wodurch eine Hochrüstung per Software anstelle stets neuer Antennen-Hardware ermöglicht wird. Dadurch ist die Hinzunahme neuer oder Änderung genutzter Frequenzen nicht mehr hardware-gebunden, also leichter durchführbar. WiMAX definiert eine verbindungsorientierte (!) MAC-Ebene, die nicht nur auf IP-Daten sondern auch auf leitungsvermittelte klassische Telefonie (TDM / PSTN) abzielt. Der Standard definiert garantierte Dienstgüte und stellt eine Beibehaltung der Sendereihenfolge über Funkverbindungen sicher. Als Sicherheits-Funktionalität ist eine PKI-basierte Authentifizierung enthalten, die in jedem Clientsystem ein digitales X.509 Zertifikat erfordert. Mit diesen Eigenschaften bietet sich WiMAX geradezu für einen nahtlosen Übergang vom wireless LAN zum wireless MAN an, mögliche Einsatzszenarios und Märkte sind in Abbildung 3.11 bis Abbildung 3.13 dargestellt. Hier wird deutlich, dass WiMAX als DSL-Alternative den SOHO-MAN-Übergang, innerstädtische Filialkonzepte, Hot Spots (heute noch WLAN-Technik) mit höherer Datenrate als WLAN und den Backbone für Mobilfunkzellen bis zum LWL-Übergang ins Internet oder Corporate Netz abdecken will.

IEEE 802.16 Standards				
Standard	802.16	802.16a	802.16-2004	802.16e
Netzwerk-Topologie	Point-to-Point und Multipoint	Point-to-Point und Multipoint	Point-to-Point, Multipoint und vermascht	Nur Multipoint
Frequenzen	10 bis 66 GHz	2 bis 11 GHz	2 bis 11 GHz	2 bis 11 GHz
Line of Sight	Erforderlich mit Freznel Clearance	Üblicherweise erforderlich	Hilfreich, aber nicht erforderlich	Nicht erforderlich
Beschreibung	Standardisierte LMDS	Basiert auf MMDS und dem eruopäischen HiperMAN System	geändertes 802.16a; Gründung von WiMAX	Erweitert 802.16-2004 um Handoff Funktionalität
Standard	2001	September 2003	Oktober 2004	Ende 2005
Produkt-Verfügbarkeit	2002	Juni 2004 (Carrier Core), November 2004 (Enterprise)	Anfang 2005 (Enterprise), Ende 2005 (SOHO)	2006 (portabel), 2007 (mobil)

Abbildung 3.10: IEEE 802.16 Standards und technische Eckwerte

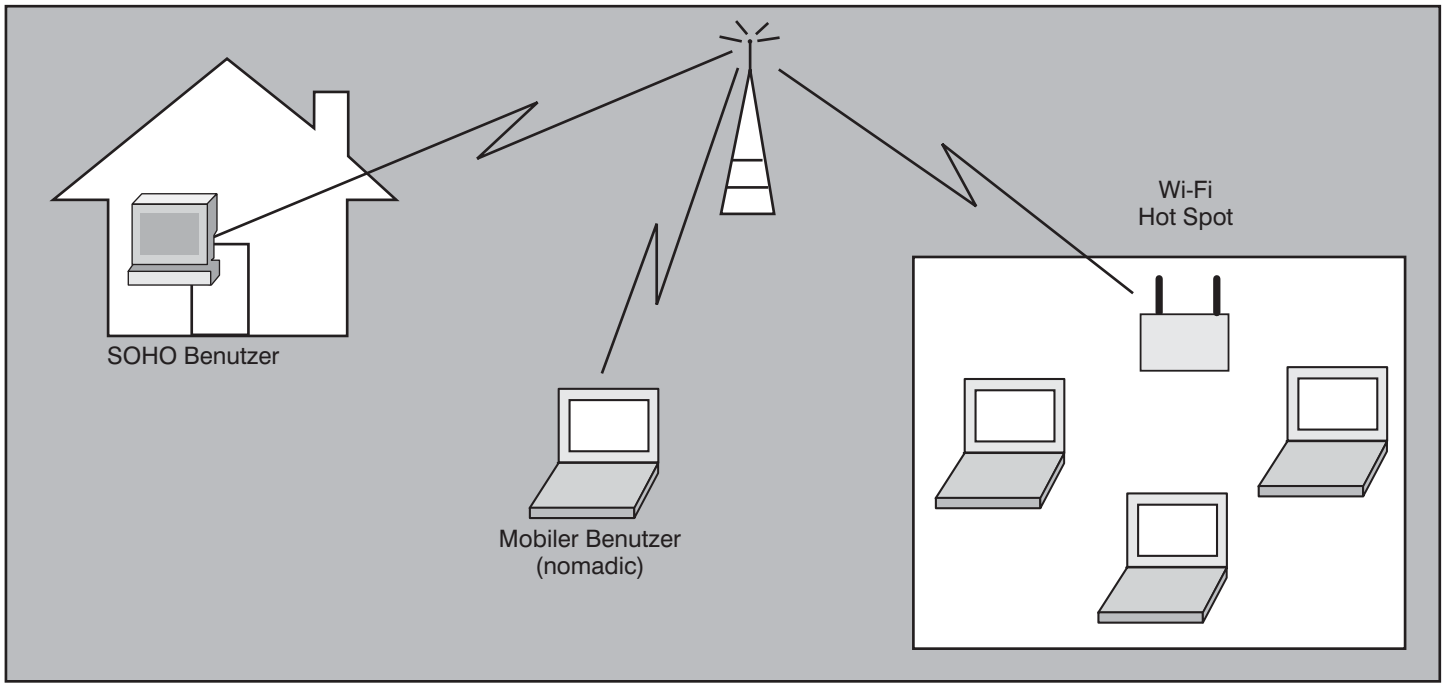


Abbildung 3.11: Einfaches WiMAX Einsatzszenario

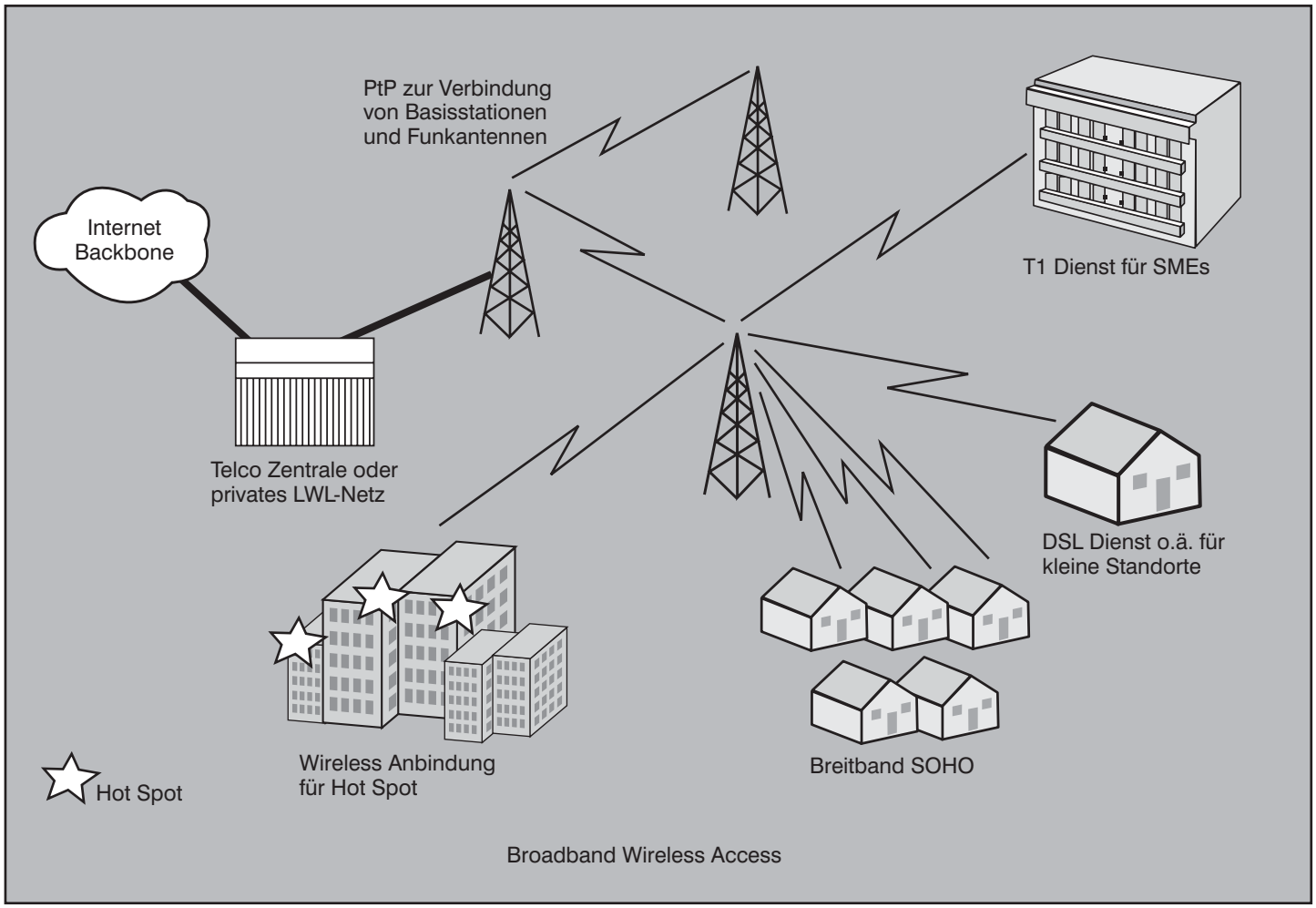


Abbildung 3.12: WiMAX Architektur und Einsatzbereiche

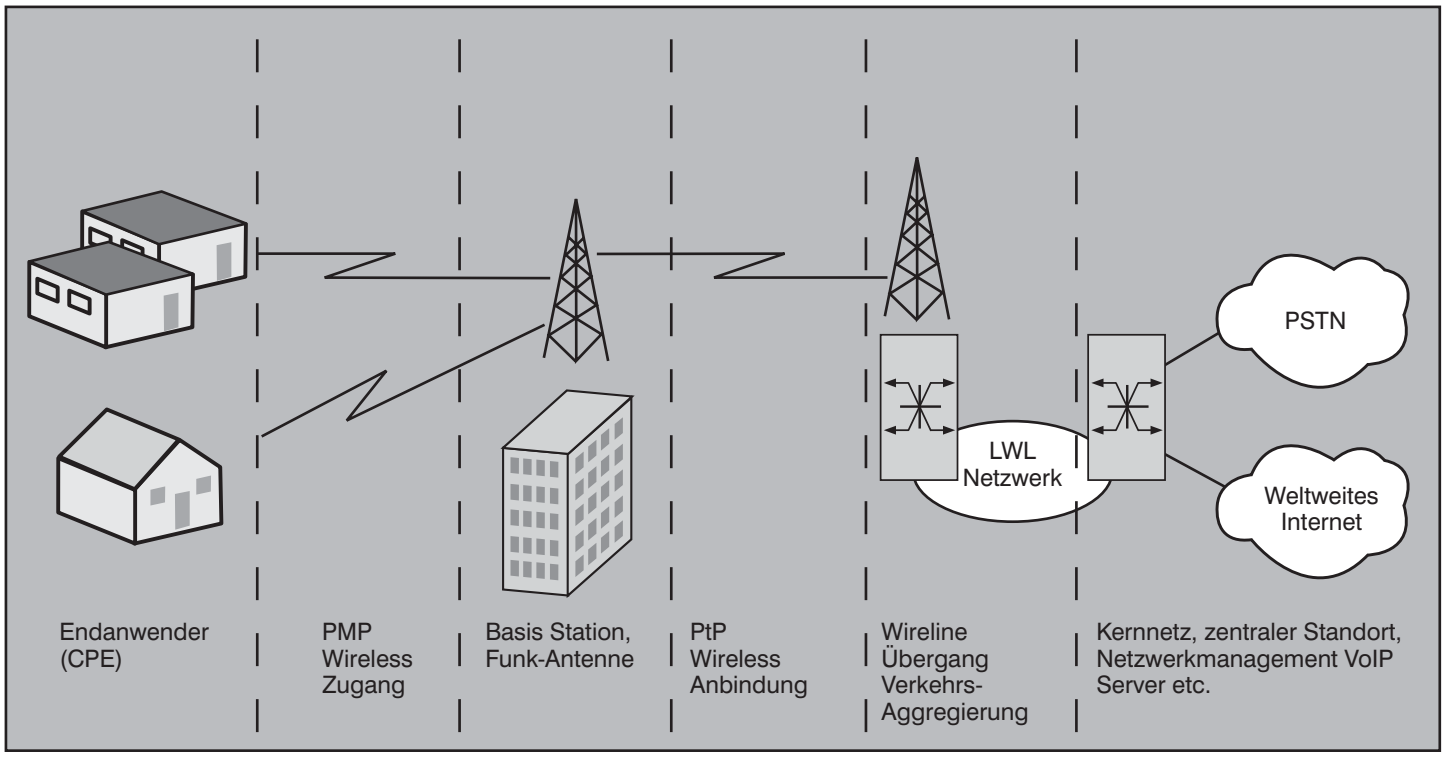


Abbildung 3.13: WiMAX Einsatzbereiche, Komponenten, Märkte

3.4 Friedliche Koexistenz?

Eine Anmerkung kann an dieser Stelle sicher getroffen werden: Alle drei Wireless Arbeitsgruppen 802.16, 802.20 und 802.22 überlappen sich in ihrer inhaltlichen Abdeckung und werden letztlich um Marktanteile konkurrieren, auch wenn alle drei aktuell von einer friedlichen Koexistenz reden. Soweit es um Schnittstellen und die Nutzung lizenzfreier Frequenzbänder geht, gibt zudem Überschneidungen mit 802.11 und 802.15. Alle Gruppen haben daher in irgendeiner Form Abstimmung und Regelungen auf der ToDo Liste stehen, um solche Interferenzen zu vermeiden oder zu beseitigen:

- 802.11k: Funkmessungen zur Vermeidung von Interferenzen zwischen benachbarten AP's
- 802.15.2: Koexistenz zwischen 802.11 und 802.15 (Bluetooth) oder ZigBee im 2,4 GHz Band
- 802.19: Allgemeine Koexistenz aller IEEE Wireless Netze, so dass Wi-Fi, Bluetooth, WiMAX/802.16 und Mobile-Fi (802.20) zusammen arbeiten können.
- 802.21: Roaming zwischen verschiedenen Netztypen, Ethernet (802.3), 3G Mobilfunk und 802 Wireless
- 802.22: Könnte die Basis eines allgemeinen Systemverfahrens werden, um freie Kanäle / Bandbreite zu finden und zu nutzen

Eine Übersicht der verschiedenen Bereiche und der zuständigen Standardisierungsgruppen ist in Abbildung 3.14 dargestellt.

Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

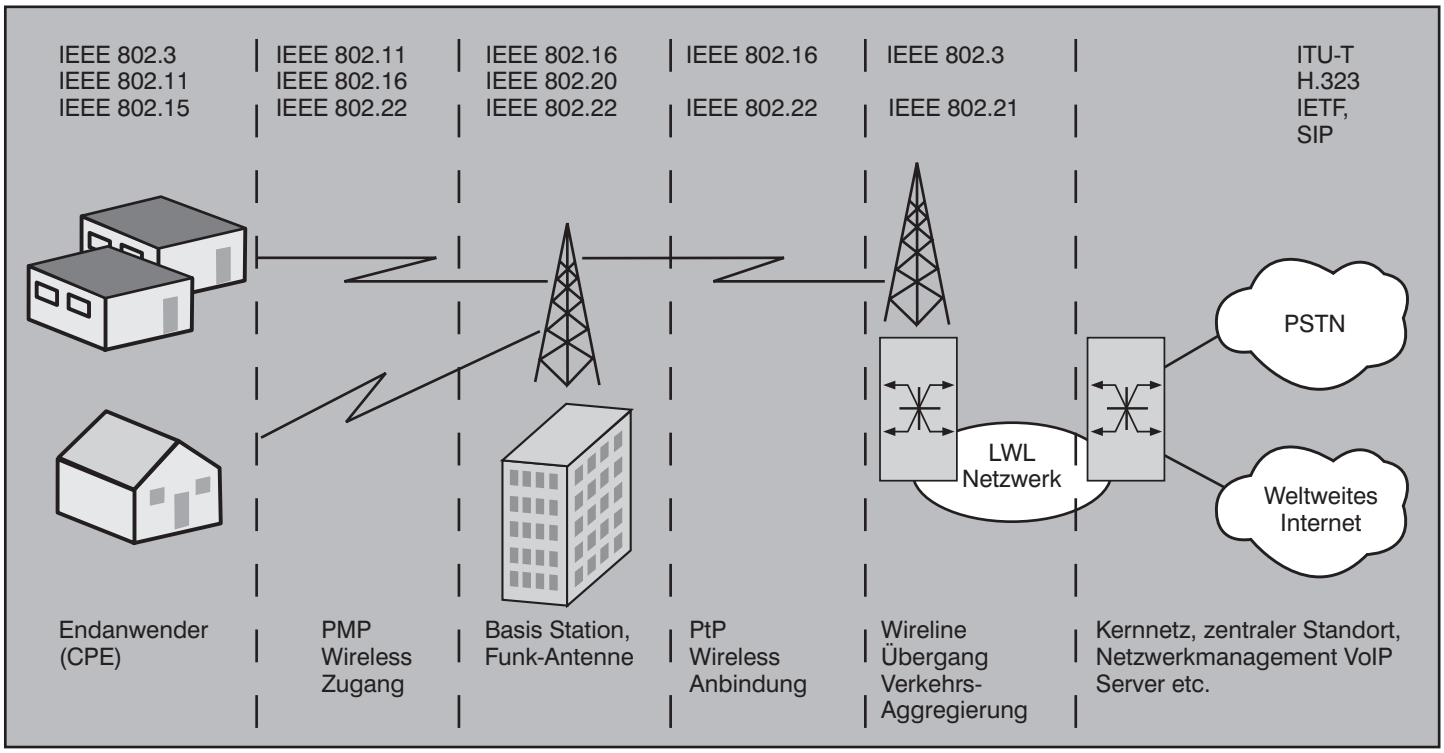


Abbildung 3.14: Netzbereiche und Standardisierung

Abkürzungen

AC	Access Controler
AES	Advanced Encryption Standard
AP	Access Point
BOF	Birds Of a Feather
BWA	Broadband Wireless Access
CAC	Call Admission Control
CAPWAP	Control and Provisioning of Wireless Access Points
CCX	Cisco Compatible Extensions
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
FAST	Flexible Authentication von Secure Tunneling
GSM	Global System for Mobile Communication
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight EAP
LMDS	Local Multipoint Distribution System
LWAPP	Light Weight Access Point Protocol
MAC	Media Access Control
MBWA	Mobile Broadband Wireless Access
MD5	EAP Message Digest 5
MMDS	Multichannel Multipoint Distribution System
MS-CHAP	Microsoft-CHAP
NIC	Network Interface Card
OEM	Open Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PEAP	Protected EAP Protocol
PKI	Public-Key-Infrastructur
PMP	Punkt-zu-Multipunkt
PSK	Pre-Shared Key
PSTN	Public Switched Telephony Network
PTP	Punkt-zu-Punkt
RADIUS	Remote Authentication Dial In User Service
SDR	Software Defined Radio
SPoF	Single Point of Failure
SVP	SpectraLink Voice Priority
TDM	Time Division Multiplexing
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
TPC	Transmit Power Control
TTLS	Tunneled TLS
UHF	Ultra High Frequency
VHF	Very High Frequency
VoWLAN	Voice over WLAN
VRRP	Virtual Router Redundancy Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WLS	Wireless LAN Switch
WLSE	Wireless LAN Service Engine
WLSM	Wireless LAN Service Module
WME	Wi-Fi Multimedia Extensions
WMM	Wi-Fi Multimedia Extensions
WPA	Wi-Fi Protected Access
WTP	Wireless Termination Point

Links

www.alcatel.de
www.bbwexchange.com
www.ieee.org/11
www.ieee.org/15
www.ieee.org/16
www.ieee.org/20
www.ieee.org/22
www.nwfusion.com
www.wimaxforum.org
www.wimedia.org
www.zigbee.org

Die Fortsetzung folgt in einem der nächsten Netzwerk Insider.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
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

Internetworking
06.06. - 10.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
14.11. - 18.11.05 in Bonn

Ethernet Technologien - neuester Stand
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.--)

Jetzt mit ipod Shuffle bis zum 31.03.05

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
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
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
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 € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

Jetzt mit ipod Shuffle bis zum 31.03.05

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
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
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
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.--)

Jetzt mit ipod Shuffle bis zum 31.03.05

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

Impressum

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

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie