ComConsult Research

Der Netzwerk Insider

Dezember 2006

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

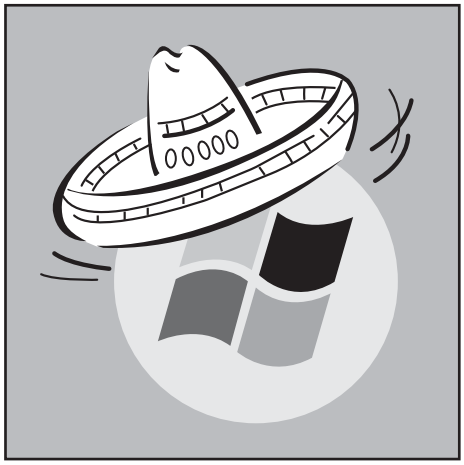
Hasta la VISTA Windows XP!

Mehrwertpotentiale von Windows Vista unabhängig betrachtet

von Markus Holländer, Dipl.-Inform. Michael van Laak

Für viele Administratoren und auch Benutzer liegt die Einführung von Windows XP noch gar nicht so lange zurück. Zugegeben - Microsoft hat XP bereits Anfang 2002 veröffentlicht und bis zur Einführung von Vista in 2007 sind dann ja schon gut 5 Jahre vergangen, doch viele Unternehmen haben diesen Schritt - wenn sie ihn denn gemacht haben - erst in den letzten Jahren vollzogen. Insofern stellt sich einmal mehr die Frage „Warum sollen wir denn zu Vista wechseln?“.

Dieser Artikel beschäftigt sich mit einigen Features von Vista, bei denen Mehrwertpotentiale vermutet werden. Hierbei werden in erster Linie das Deployment von



Vista, die Festplattenverschlüsselung und die Gruppenrichtlinien betrachtet. Ebenso wird allerdings auch das allgemeine „look-and-feel“ bewertet. Die Betrachtung beruht zu einem Teil auf Erfahrungen aus dem Testcenter des Competence Center Backoffice der ComConsult Beratung und Planung GmbH, aber auch auf dem täglichen Umgang mit dem Produkt. Erste Versuche, Vista im täglichen Betrieb einzusetzen, erfolgten mit Veröffentlichung der Beta 2. Wir möchten nicht sagen, dass die Versuche kläglich scheiterten, doch stellte sich ziemlich schnell heraus, dass man sich zwar neue Funktionalitäten anschauen konnte, aber so ein „richtiges“ Arbeiten nicht möglich war.

weiter auf Seite 23

Zweitthema

WLAN Maschen-Netze ante portas!

von Dr. Franz-Joachim Kauffels

Maschen-Netze sind eine äußerst attraktive Variante drahtloser Netze. Hat man ihre grundsätzliche Arbeitsweise erschlossen, hat die Konstruktion einen erheblichen Charme. Es gibt zwei wesentliche Standards, IEEE 802.16a im Umfeld von WiMAX und den aktuellen Draft IEEE 802.11s aus August 2006 im gewohnten WLAN-Kontext. In diesem Artikel wird speziell IEEE 802.11s untersucht, in einem Folgeartikel folgt die 16a-Variante.

1. Einführung

Zweck eines WLAN-Maschen-Netzes ist der Aufbau einer kabellosen Anbindung von Access Points bis hin zur vollständigen kabellosen Infrastruktur für die Kommunikation. Generell kann man sagen, dass Maschen-Netze als Erweiterung der bisherigen Wireless-Distribution-Systeme WDS immer dann zum Einsatz kommen können, wenn aufgrund der Historie der Umgebung keine bzw. keine flächendeckende Verkabelung vorhanden ist.

weiter auf Seite 7

Top Veranstaltung

Netzwerk-Redesign Forum 2007

auf Seite 5

Zum Geleit

SIP und Microsoft verändern den Telefonie-Markt! Haben die traditionellen Anbieter noch eine Chance?

auf Seite 2

Report des Monats

Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

auf Seite 20

Zum Geleit

SIP und Microsoft verändern den Telefonie-Markt! Haben die traditionellen Anbieter noch eine Chance?

Das ComConsult-Voice-Forum im November war geprägt von vielen Diskussionen, sowohl in der Veranstaltung als auch in den Pausen und in der Ausstellung. Zu gravierend waren die vorgestellten Analysen, zu umfangreich die Änderungen in Produkten und Technologien, die sich aktuell abzeichnen. An dieser Stelle möchte ich nun angesichts des begrenzten Umfangs eines Geleit-Worts nur zwei Aspekte herausgreifen, den Trend zum SIP-Standard und den Einstieg Microsofts in den Markt.

„Der Weg geht zur Software und weg von Hardware-basierten Lösungen“. Klarer hätte es der CTO von Siemens-Com, Rudolf Bitzinger, nicht ausdrücken können. Die Internationalisierung der Lösungen, flexible Anpassung an neue Trends in Kombination mit der Senkung der Entwicklungs- und Pflegekosten produzieren dabei einen erheblichen Druck auf die Hersteller, diesen Übergang eher heute als morgen zu machen. Die damit verbundenen Wettbewerbsvorteile können so erheblich sein, dass sie die Frage, wer den jetzt anlaufenden Verdrängungswettbewerb verlieren wird, in der Software-Frage entschieden wird. Diese Entwicklung läuft klar gegen den aktuellen Marktstatus, dass momentan noch deutlich mehr Hybridlösungen als Software-Lösungen verkauft werden.

Aber die Präsentationen der meisten Hersteller machten klar, dass die Hybridwelt ein Auslaufmodell ist und dass der End-of-Life-Termin näher ist als viele vermuten (natürlich ist die Wartung und Pflege der Hybridanlagen für die nächsten 10 Jahre gesichert). Speziell in Deutschland wurde der Übergang zu reinen Software-Lösungen bisher von der Siemens-Produktsituation blockiert. Da die HiPath 8000 bisher noch nicht massentauglich war, hat sich Siemens bisher bemüht, weiter die HiPath 4000 hochzuhalten. Hinzu kommt, dass dies im Hause Siemens ein politisches Thema ist und noch viele Mitarbeiter und Führungskräfte an der alten Welt hängen. Der Vortrag von Rudolf Bitzinger machte aber klar, dass mit der Marktreife der HiPath 8000 der strategische Schwer-

punkt seitens Siemens auf dieser Anlage liegt und liegen muss. ComConsult-Research rechnet momentan damit, dass bereits mit dem Wechsel zum Releasestand 3.0, der für Ende Q1/2007 erwartet wird, der Schwenk im Siemens-Vertrieb zur HiPath 8000 erfolgt.

Wer heute Software sagt, der meint SIP, den aufkommenden Standard für Sprach- und Multimedia-Kommunikation. Der Wechsel von Cisco von Skinny zu SIP und der Übergang bei Siemens mit der HiPath 8000 sind nur Beispiele für diesen Trend. Speziell bei den kleineren Lösungen werden Produkte wie Asterisk den Markt in den nächsten Jahren verändern. Betrachtet man das momentane Preisniveau der Einstiegslösungen von Nortel mit dem BCM und entsprechende Produkte von Innovaphone, nur um Beispiele zu nennen, dann muss man feststellen, dass diese Marktveränderung schon mehr als begonnen hat. Nach wie vor sind die Preise bei Hardware-Telefon-Endgeräten zu hoch, aber gerade hier wird der Wechsel zum Standard vieles bewegen. Produkte wie der BCM von Nortel sind noch aus anderer Sicht spannend. Mal abgesehen von der sonstigen Funktionalität decken sie den vollen Umfang eines SIP-PSTN-Gateways mit Doppel-S2M- Schnittstelle ab. Das für einen Preis ab 1000 Euro. Daraus schließe ich sofort, dass jedes SIP-PSTN-Gateway, das teurer ist, einfach zu teuer ist.

Nortel zeigt mit dem BCM eindeutig, dass ein leistungsfähiges Gateway nicht teurer als 1000 Euro sein muss. Mit dem Übergang auf einen offenen Standard werden und müssen Preise für Komponenten wie Gateways und Telefone wegbrechen.

Umso entscheidender ist es, dass mit dem SIP-Standard auch interoperable Lösungen entstehen. Dies ist mitnichten der Fall und hier ist der Anwender gefragt. Viele Hersteller argumentieren gerne, dass der SIP-Standard nicht genügend Funktionalität hergibt und deshalb herstellerspezifische Ergänzungen erforderlich sind. Klare Aussage von mir: das ist eine absichtliche und klare Lüge! Wir haben das Problem, dass viele der weitergehenden Funktionen sich in einem Draft-Zustand befinden und der Standard nicht abgeschlossen ist. Aber wer den Vortrag von Frau Borowka über SIPPING gehört hat und den damit verbundenen Funktionsumfang realisiert hat, der hat auch erkannt, dass das Gerede von Funktionsdefiziten auf der SIP-Seite Unfug ist. Bezeichnend war die Reaktion der Hersteller auf die Aufforderung von Frau Borowka, doch bitte die Funktionsmerkmale zu benennen, die unter Berücksichtigung von SIPPING nicht abgedeckt sind. Keiner der anwesenden Hersteller (und das waren fast alle namhaften) war dazu in der Lage. Gerne nehmen wir die Kommentare der Hersteller zu diesem Thema entgegen und veröffentlichen diese.

Um das noch einmal zu wiederholen: SIP liefert keine Magerlösung, die der zwingenden Ergänzung durch die Hersteller bedarf. Der Standard mit allen zugehörigen RFC´s und Drafts deckt den vollständigen Umfang einer professionellen Telefonie-Lösung ab. Durch die Integration von Instant Messaging, Präsenz, Video und Multimedia geht der Standard in der Realität noch weit über den Funktionsumfang traditioneller Lösungen hinaus. Der Anwender ist in Zukunft gefordert. Akzeptiert er, dass ihm die Hersteller abgewandelte und proprietäre SIP-Funktionen aufzwingen, die eben keinen Mix mit Produkten anderer Hersteller gestatten, dann ist er selber schuld.

SIP und Microsoft verändern den Telefonie-Markt! Haben die traditionellen Anbieter noch eine Chance?

SIP ist nicht frei von Tücken, das zeigte der Erfahrungsbericht der Commerzbank auf dem Voice-Forum. Unabhängig von dem eingesetzten Produkt hat SIP einige unvermeidbare Merkwürdigkeiten in der Handhabung. Aber dies ist eine Gewöhnungssache seitens der Anwender und kein unüberwindliches Hindernis.

ComConsult Research wird den Anwender bei der Auswahl von SIP-Lösungen aktiv und massiv unterstützen. Zum ComConsult-Netzwerk-Redesign-Forum 2007 stellen wir exklusiv unseren Leitfaden „Einstieg in standardisierte Kommunikations-Lösungen“ vor. Wir stellen uns zu 100% als Unternehmen hinter standardisierte Lösungen und wehren uns gegen alle Versuche, hier den Anwender zu hintergehen.

Und hier kommt Microsoft ins Spiel. Der Einstieg von Microsoft in den Sprachmarkt verändert in seinen Detailfacetten unendlich viel. Er wird zum kompletten Umbruch des Marktes führen, auch wenn das noch nicht viele so sehen. Aus der Diskussion auf dem ComConsult-Voice-Forum war zu entnehmen, dass sich viele Teilnehmer des angekündigten Funktionsumfangs nicht im Klaren waren. Microsoft hat bereits den Umfang des Folgereleases aus 2008 angekündigt. Während die erste Version im Jahr 2007 ca. 27 Funktionsmerkmale haben wird, wird im Folgerelease der OCS komplett mit dem Nortel MCS integriert. Zusammen mit Exchange 2007 wird ein Funktionsschuh daraus, der sehr ernst zu nehmen ist.

Aber das ist im Grunde genommen unwichtig. Der spannende und den Markt verändernde Part im Einstieg von Microsoft liegt im Client. Mit dem Übergang zum Unified Client, einem Soft-Client, der die komplette Kommunikationsfunktionalität von der Sprache über IM, Mail, Video bis hin zur Kollaboration enthält, erfolgt ein Umbruch im Markt. Betriebssysteme der Zukunft, dazu gehört auch Apples OSX 10.5, das für März 2007 erwartet wird, integrieren komplette Kommunikationsoberflächen in einer Form, dass die Nutzung dem Anwender quasi aufgedrängt wird, sie wird Teil seiner täglichen Arbeit in der jeweiligen Betriebssystem-Umgebung.

Konsequenzen?

Zwei Wesentliche aus unserer Sicht:

- Trotz der ungewöhnlichen Umsetzung von SIP auf TCP-Basis, die allerdings im Standard erlaubt ist, fördert Microsoft die Verbreitung von SIP. Dies ist einer der Faktoren, der aus unserer Sicht für eine beschleunigte Einführung von SIP in die Unternehmen sorgen wird
- Microsoft verschiebt den Schwerpunkt vom Hardware-Telefon zum Soft-Client. Wir werden auch in Zukunft ein Hardware-Telefon haben, aber dessen Design wird mehr vom individuellen Geschmack abhängen. Dies wird in den nächsten 2 bis 3 Jahren erfolgen. Interessanterweise ist dieser Trend nicht auf Microsoft beschränkt. Mehrere andere Hersteller, darunter massiv Cisco Systems, forcieren den Grundgedanken des Unified Clients, also der Integration mehrerer Kommunikationsfunktionen in einen Clienten. Konzeptionell muss dies angesichts der bestehenden Bedeutung von Email und der zunehmenden Bedeutung von Instant Messaging bei einem Software-Client auf der PC-Seite enden

Wie weit ist die Microsoft-Entwicklung technisch ernst zu nehmen unabhängig von strategischen Erwägungen?

Das Research-Team der ComConsult Beratung und Planung hat dies seit mehreren Monaten evaluiert. Auch wenn die Produkte zum Teil bisher nur in frühen Betaversionen verfügbar sind, so ist doch die Meinung im Analyseteam nach anfänglich sehr kontroversen Diskussionen klar:

Die Microsoft-Lösung wird eine ernst zu nehmende Alternative auch für die reine Sprachkommunikation!

Nachdem diese Sichtweise auf dem ComConsult-Voice-Forum deutlich vertreten wurde, wogte die Diskussion in den Pausen und durch die Aussteller. Viele Teilnehmer gerade aus den großen Unternehmen wollten dieser Sichtweise nicht folgen oder waren doch zumindest deutlich irritiert.

Was nun? Nun, wir arbeiten weiter an dem Thema. Zum ComConsult Netzwerk-Redesign-Forum im April 2007 werden wir die nächste Stufe der Analyse- und Testarbeiten abgeschlossen haben. Diese Ergebnisse werden exklusiv auf dem Forum präsentiert.

Was können Sie tun?

Die aktuelle technische Entwicklung erfordert für jedes Unternehmen einen Rahmenstandard und klare Aussagen zur Positionierung Ihres Unternehmens zu den aufkommenden neuen Kommunikationstechnologien:

- Wie stehen Sie zum Grundgedanken des Unified Client?
- Wie stehen Sie zu SIP als Standard und welche Schlussfolgerungen ziehen Sie daraus für Ihre künftige Produktauswahl?
- Welchen Stellenwert hat Instant Messaging für Sie in Zukunft?
- In welchem Umfang werden Sie die neuen Kollaborations-Funktionen ein-

führen?

- Werden Sie Web-Konferenz-Technologien nutzen?
- Wie stehen sie zu Präsenz-Technologien?
- Wo stehen Ihre Infrastrukturen? Sind Ihre IP-Adressräume, Ihr DNS, Ihr DHCP auf die massiven Erweiterungen, die auf Sie zukommen, vorbereitet? Wo stehen Ihre Verzeichnisdienste? Wie kombinieren Sie in Zukunft diese Verzeichnisdienste? Macht der Microsoft-Weg in eine integrierte Lösung für Verzeichnis- und IP-Dienste doch vielleicht Sinn?

Das sind nur einige der Fragen, denen Sie sich aus unserer Sicht stellen müssen. Und eine Umsetzung der Antworten als Rahmenstandard für Ihr Unternehmen ist unverzichtbar, soll es nicht zu einem Wildwuchs an Lösungen kommen, der angesichts der Einbettung der neuen Funktionen auf Betriebssystemebene sonst vorprogrammiert ist.

Ist die Sichtweise, dass die traditionellen Hersteller gefährdet sind, übertrieben?

Überlegen Sie einmal, was aus ehemals komplexen Produkten wie Switch-Systemen geworden ist, die Sie heute in jedem Media-Markt in großer Auswahl kaufen können. Nehmen Sie sich doch einmal eine Netgear-Konsumer-Firewall der High-end-Seite. Derartige Produkte waren vor 10 Jahren unendlich teuer und wurden durch Spezialisten bedient. Wie viele Linux-Bastler haben denn heute schon Asterisk installiert? Haben Sie sich einmal mit den Einstiegs-TK-Lösungen befasst? Nortel hat inzwischen mehr als 100.000 BCM verkauft (und das Produkt ist nicht trivial zu konfigurieren), der Vertrieb läuft inzwischen über Elektriker vor Ort, die auch den Service übernehmen (spannendes Erlebnis, wenn der Handwerker, der sich gerade mit einem neu zu verlegenden Kabel durch den Dachstuhl ihres Privathauses quält, auf einmal mit Ihnen eine Diskussion über IP-Telefonie-Anlagen startet und versucht, Ihnen einen BCM zu verkaufen).

Wenn es möglich ist, Produkte wie die Fritz!Box von AVM und den 1723 von Lancom im Konsumer-nahen Bereich zu vermarkten, was bedeutet das denn für den Unternehmensmarkt in einigen Jahren? Hier ist doch eindeutig etwas in Bewegung, vor dem man nicht die Augen schließen kann. Beobachten Sie doch einmal in den nächsten Monaten die Weiterentwicklung der grafischen Konfigurations-Oberflächen für Asterisk, dies wird Ihnen einen Vorgeschmack auf das Kommende geben.

Mit der Änderung der Kommunikations-Produkte im Preis kommt automatisch die begleitende Änderung der Vertriebswege.

Das mag für die Top 100 der deutschen Industrie, die wir alle so lieben und die wir gerne immer als Referenz anführen, egal sein. Aber der TK-Markt wird nicht durch die Top 100 geprägt. Hier ist sowieso kaum Geld zu verdienen. Der Markt der Zukunft liegt aus meiner Sicht für die Hersteller klar bei den kleinen und mittelgroßen Unternehmen. Ihr Unternehmen mag ja nicht zu diesem Kreis der kleinen Kunden gehören, aber der Sie beliefernde Hersteller hängt in seinem Überleben davon ab, ob er sich diesen Markt erschließen kann.

Und hier schließt sich der Kreis. Wenn Sie den internationalen Markt in den letzten Monaten gut beobachtet haben, dann haben Sie einen deutlichen Schwenk hin auf diesen Markt mindestens bei einem Hersteller bemerkt. Dieser Hersteller heißt Cisco Systems. Die Strategie von Cisco steht in einem krassen Widerspruch zum Vorgehen von vielen anderen Herstellern, die ihren persönlichen Schwerpunkt immer noch auf der Großkundenseite sehen. Cisco war in der Vergangenheit nun nicht so schlecht darin, wichtige Trends zu erkennen und ihnen zu folgen.

In der Kombination dieser Faktoren beginnend aus dem Einstieg von Microsoft und endend bei sinkenden Preisen und sich wandelnden Vertriebswegen liegt der aktuelle Sprengstoff im Markt. Und so leid mir das tut, meine persönliche Erwartung ist, dass mindestens einer der ganz Großen das nicht überleben wird. Je kritischer der Markt wird, desto mehr werden die schon begonnenen Allianzen und Übernahmen eine Rolle spielen. Aus diesem Grund ist mit dieser Aussage auch keinerlei Spekulation auf einen bestimmten Hersteller verbunden. Die Herstellerlandschaft wird sich in den nächsten Jahren ändern müssen und es ist schwer vorhersehbar, was dabei alles passieren kann.

Wir freuen uns darauf, diese Themen mit Ihnen auf dem ComConsult-Netzwerk-Redesign-Forum 2007 diskutieren zu können. Schon jetzt ist klar, das wird unsere wichtigste Veranstaltung seit Jahren, da sich gleichzeitig auf der Netzwerk- und Infrastrukturseite erhebliche Veränderungen ergeben.

In diesem Sinne
Ihr
Team von ComConsult Research

Dr. Jürgen Suppan

Aktueller Kongress

Netzwerk-Redesign Forum 2007

Die ComConsult Akademie veranstaltet vom 23. - 26.04.2007 ihren Kongress „Netzwerk-Redesign Forum 2007“ in Königswinter.

Wir stehen vor gravierenden Änderungen im Bereich der Netzwerk-Technologien und vor allem in den Applikations-Architekturen, die mit Netzwerken realisiert werden. Dies wird zu einem umfassenden Bedarf an Neukonfiguration über alle Layer des Referenzmodells führen.

Das Netzwerk-Redesign-Forum 2007 ist unsere zentrale Veranstaltung des Jahres 2007, die sich intensiv den Änderungen der Netzwerk-Technologien und dem damit verbundenen Einfluss auf das Design und den Betrieb der Netzwerke widmet.

ComConsult-Research hat eine große Markt- und Technologie-Analyse gestartet, die die Grundlage für das Netzwerk-Redesign-Forum 2007 bilden wird.

Unter anderem werden wir auf folgende Entwicklungen eingehen:

- WAN-Konvergenz durch immer mehr Bandbreite
- Service-orientierte und Standort-neutrale Architekturen
- Von der Sprachkommunikation zur Kollaboration
- IP-Infrastrukturen im Wandel
- Sicherheits-Konzepte
- Quality of Service
- Wireless LAN: 11n und Mesh in der Analyse
- Auswahl neuer Netzwerk-Komponenten

Diese Liste ist noch nicht vollständig. Aber sie zeigt bereits, wie heiß die Themen des Netzwerk-Redesign-Forums 2007 sind. Bereits jetzt steht fest, dass dies eine der weitgehendsden Veranstaltungen seit Jahren werden wird.

Das Netzwerk-Redesign-Forum 2007 ist für jeden Planer und Betreiber von Netzwerken ein Muss.

In den letzten Jahren war diese Veranstaltung immer ausgebucht.

Als Dankeschön für die vertrauensvolle Zusammenarbeit gewähren wir Ihnen dabei bis zum 31.12.2006 den einmaligen Sonderrabatt von fast 10%.

Zögern Sie nicht und sichern Sie sich einen Platz auf unserer Top-Veranstaltung des Jahres 2007.

Die Moderation dieses Kongresses leitet Dr. Jürgen Suppan.

Dr. Jürgen Suppan gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt. Seine Seminare zählen durch ihren didaktischen und lebendigen Aufbau und ihre Praxisnähe und Herstellerneutralität zu unseren erfolgreichsten Veranstaltungen.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-phase bis 31.12.2006

Anmeldung
Netzwerk-Redesign Forum 2007

Frühbucher-phase bis 31.12.2006

☐ Ich buche den Kongress
Netzwerk-Redesign Forum 2007
vom 23.04. - 26.04.07 in Königswinter
inkl. Intensiv-Training am ersten Tag
zum Preis von € 1.990,-* zzgl. MwSt.

☐ vom 24.04. - 26.04.07 in Königswinter
ohne Intensiv-Training am ersten Tag
zum Preis von € 1.590,-* zzgl. MwSt.

*Preise gültig bis 31.12.2006

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

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

Neue Veranstaltung

Neues Seminar: Windows Vista - Tatsächlich Mehrwerte vorhanden?

Die ComConsult Akademie veranstaltet am 07. Februar 2007 erstmalig ihr neues Seminar „Windows Vista - Tatsächlich Mehrwerte vorhanden?“ in Köln.

Microsoft hat Ende November 2006 die finale Version von Windows Vista freigegeben und stellt diese auch für Unternehmenskunden zur Verfügung. Ende Januar 2007 kommt Vista dann in den Handel. Was haben Unternehmen von dieser neuen Version des führenden Betriebssystems zu halten? Schafft es Microsoft, mit der Etablierung von Vista die Basis für seine „people ready software“ zu legen? Welche Mehrwertpotentiale bietet Vista, insbesondere wenn man schon Windows XP im Unternehmen eingeführt hat? Competence Center Leiter Markus Holländer und Dipl.-Inform. Michael van Laak - die technisch Verantwortlichen der ComConsult Beratung und Planung GmbH zu dieser Thematik - erläutern diese Fragen in dem vorliegenden Seminar für Entscheider. Es werden insbesondere die Funktionen und Dienste betrachtet, die einen Mehrwert versprechen. Es ist vorgesehen, dass beide Spezialisten vor Ort sind.

Dabei greifen die Experten u.a. auch auf die persönliche Arbeit mit Vista seit der Beta-Veröffentlichung zurück. Kombiniert mit der Erfahrung zahlreicher Projekte im Windows Umfeld bis hin zu einem weltweiten Rollout von Windows XP erfolgt eine kritische Betrachtung des Produkts. Auch werden die anhängigen Produkte wie 2007 Microsoft Office System, Exchange Server 2007, Office Communication Server 2007 und Longhorn Server hinsichtlich ihrer technischen Interaktion aber auch der strategischen Auswirkung betrachtet.

In diesem Seminar

- lernen Sie
  - verschiedenste Neuerungen von Vista kennen
  - die Mehrwertpotentiale von Vista einzuschätzen
  - die Risiken mit oder von Vista einzuordnen
  - die Key-Features von Vista für Ihr Unternehmen zu erkennen
  - die Schnittstellen von Vista zu anderen Applikationen einzuschätzen
- erfahren Sie
  - die Einschätzung der unabhängigen Spezialisten zur Microsoft Strategie
  - die Einschätzung der unabhängigen Spezialisten hinsichtlich von Abhängigkeiten zu anderen Applikationen
- diskutieren Sie
  - mit anderen Teilnehmern und den Spezialisten über die gesamte Thematik

Referenten dieses Seminars sind Markus Holländer und Dipl.-Inform. Michael van Laak von der ComConsult Beratung und Planung GmbH.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Windows Vista - Tatsächlich Mehrwerte vorhanden?

☐ Ich buche das Seminar
Windows Vista - Tatsächlich Mehrwerte vorhanden?
am 07.02.2007 in Köln
zum Preis von € 990,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____07

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

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

Zweitthema

WLAN Maschen-Netze ante portas!

Fortsetzung von Seite 1

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

Beispiele sind:

- Hotels
- Krankenhäuser
- Schulen
- Bahnhöfe
- Kommerzielle Mietgebäude
- Messegelände
- Fabrikanlagen
- Hafengelände
- Flughäfen
- Schiffe

Gerade auch für hochverfügbare RFID-Logistik-Anwendungen bietet diese Technologie die ideale Ergänzung. Hinzu kommen Anwendungen im Bereich Katastrophen-Einsatz im Falle zerstörter Infrastrukturen (hier in Kombination mit Sprachanwendungen zum Aufbau eines temporären Telefonienetzes, siehe dazu bestehende Access-Point-GSM-Kombinationen).

Es gibt in einem Wireless Maschen Netz folgende grundsätzliche Komponenten:

- Maschen-Knoten, die die gesamte Logik des Maschen-Netzes unterstützen und in der Lage sind, sich mit anderen Maschen-Knoten zu einem geschlossenen Maschen-Netz zusammenzufinden

- Maschen Access Points, die zunächst einmal die Fähigkeiten von Maschen-Knoten haben, darüber hinaus aber auch noch Access Points für Stationen sind, die nicht an der Logik des Maschen-Netzes teilnehmen können, sondern einen normalen Access Point erwarten, an dem sie sich assoziieren können

- Stationen, die keine Maschen-Fähigkeiten haben, und sich an Maschen Access Points assoziieren müssen um kommunizieren zu können

- Maschen Portale, die die Fähigkeiten von Maschen-Knoten und ggf. auch Access Point-Fähigkeiten haben und darüber hinaus in der Lage sind, einen Übergang zwischen einem Maschen-Netz und einem anderen verkabelten oder kabellosen Netz herzustellen.

Die einzige Voraussetzung für die Bildung eines vollständigen und funktionsfähigen Maschennetzes ist es, dass sich die Maschen-Knoten im funktechnischen Sinne so nahe stehen, dass sie mindestens paarweise kommunizieren können. Welche Entfernung dabei maximal zwischen zwei Maschen Knoten bestehen darf, hängt von den Umgebungsbedingungen und der verwendeten Technologie ab. Bei IEEE 802.11s senden und empfangen die Maschen Knoten mit den Radioteilen nach den Standards IEEE 802.11a,b,g,h oder zukünftig auch n in den 2,4 oder 5 Mhz-Bändern (wobei 11a spezielle Bänder mit 1 W Sendeleistung für größere Entfernungen unterstützt).

Sind nun die Maschen Knoten montiert und haben Strom, müssen sie sich zu einem Maschen-Netz organisieren. Dazu senden sie zunächst Kennungen herum, die den Zweck haben, die unmittelbaren Nachbarn zu finden. Mit diesen Nachbarn werden dann bidirektionale Verbindungen aufgebaut. Machen das alle Knoten mit allen Nachbarn, haben wir eine vollständige geschlossene Topologie mit bidirektionalen Verbindungen. (siehe Abbildungen 1-3)

Der letzte Schritt zu einem Wireless Maschen Netz ist dann die Etablierung eines Routing und eines Forwarding-Verfahrens, damit nicht nur Nachbarn unmittelbar kommunizieren können (Single Hop) son-

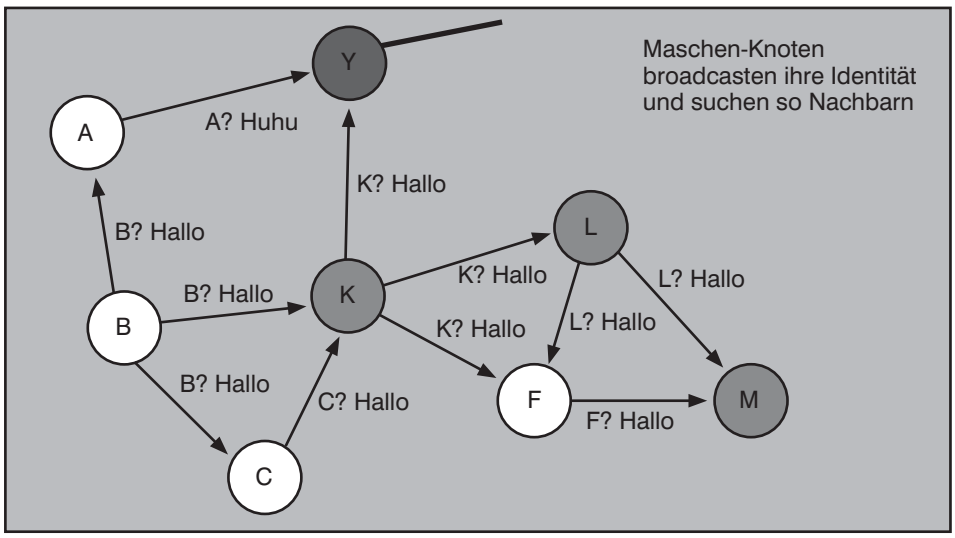


Abbildung 1: Bildung des Maschennetzes (1)

WLAN Maschen-Netze ante portas!

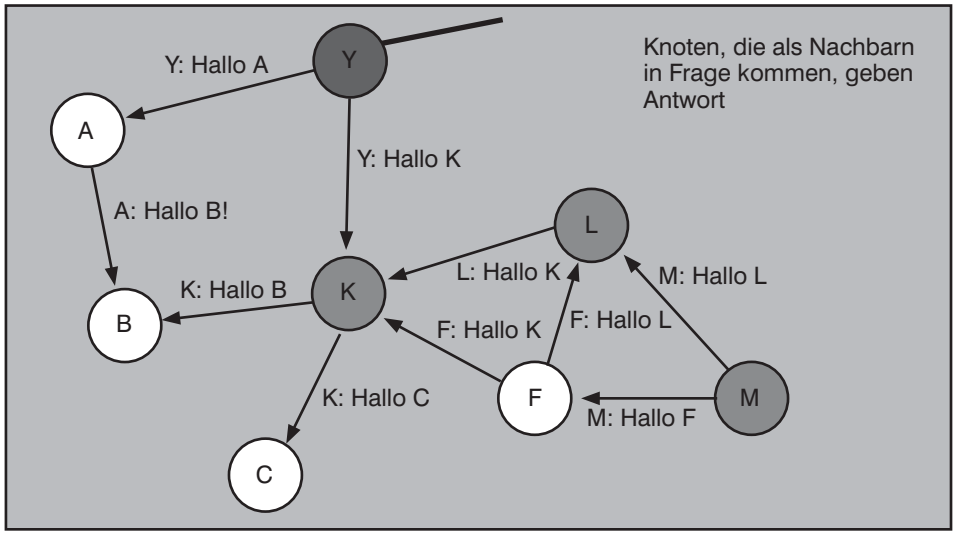


Abbildung 2: Bildung des Maschennetzes (2)

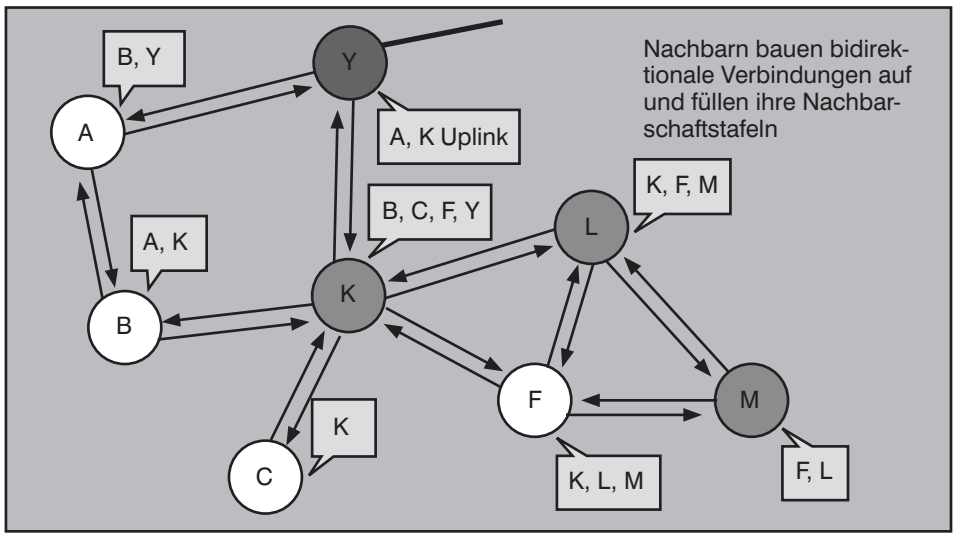


Abbildung 3: Bildung des Maschennetzes (3)

dern es auch Wege durch das ganze Netz von allen Quellen zu allen Zielen gibt (Multi-Hop). Wenn diese Verfahren dynamisch sind, können Änderungen der Topologie sofort berücksichtigt werden. Siehe dazu Abbildung 4.

Damit das Ganze auch im Zusammenwirken mit anderen Netzen und mit Schnittstellen zu höheren Protokollen reibungslos funktioniert, müssen Path Selection und Forwarding für Stationen außerhalb des Maschen Netzes vollständig versteckt werden. Also finden sie alle innerhalb des Layer 2 statt, so dass nach außen der Eindruck eines normalen konventionellen Layer-2 Subnetzes entsteht.

Aus dem bisher Gesagten kann man folgende Vorzüge von Maschen Netzen erkennen:

- ein Wireless Maschen-Netz ist aufgrund der „Selbstkonfigurierung“ ausgesprochen simpel aufzubauen
- ein Wireless Maschen-Netz ist sehr leicht zu erweitern, einfach indem man neue Maschen Knoten hinzufügt
- ein Wireless Maschen-Netz ist unempfindlich gegenüber dem Ausfall einzelner Maschen-Knoten, weil es durch Anpassung der Routen Fehlstellen automatisch überbrücken kann. Eine Grenze ergibt sich nur dann, wenn der Ausfall von Knoten bestimmte andere Knoten in die funktechnische Isolation treibt. Je nach Konstruktion entstehen dann zwei disjunkte, aber in sich funktionsfähige Maschen-Netze
- ein Wireless Maschen-Netz ist PORTABEL
- Ein Wireless Maschen-Netz kann die Nachrichtenströme unter gewissen Voraussetzungen der Verteilung von Quellen und Zielen parallelisiert abarbeiten, weil die Anzahl von gleichzeitig aktiven Routen nicht durch die Konstruktion beschränkt wird.

Zur Ausführung der Verfahren zur Routen-Ermittlung und Verwaltung wird vermutlich deutlich mehr Rechenleistung benötigt als in den bisherigen relativ einfach aufgebauten Access Points. Von daher kann nicht generell mit einer Aufrüstbarkeit bestehender Produkte gerechnet werden.

Ein anderer Aspekt ist die Verwendung mehrerer Radioteile (in der Praxis muss man davon ausgehen, dass Maschenknoten generell mehrere Radioteile haben). Bei WLAN Maschen-Netzen nach IEEE

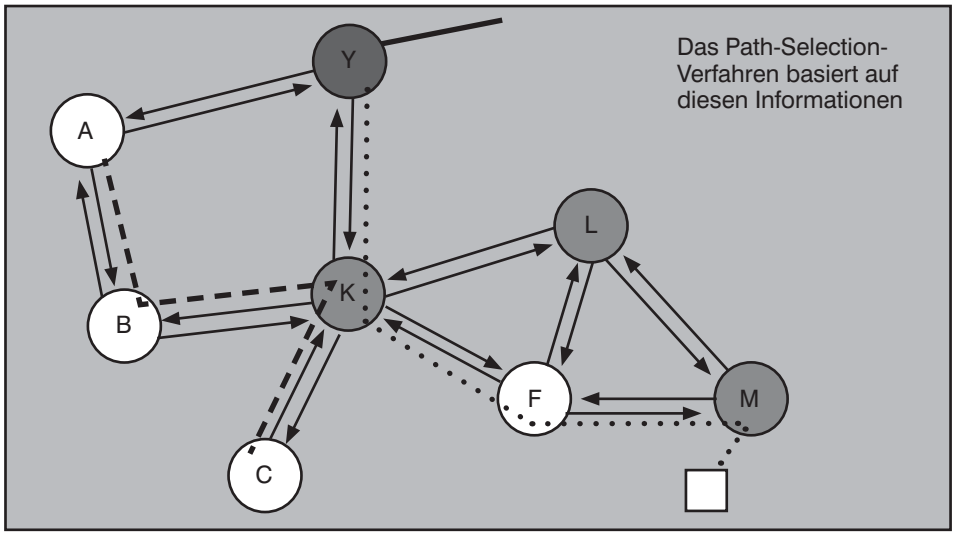


Abbildung 4: Bildung des Maschennetzes (4)

802.11s ist es nämlich so, dass die Maschen-Knoten für die Organisation untereinander und für den eigentlichen Datenverkehr unterschiedliche Kanäle benutzen können. Davon haben sie natürlich umso mehr, wenn sie nicht dauernd zwischen den Kanälen umschalten müssen. Auf diese Weise kann man, wie wir noch weiter unten sehen werden, den bislang nachteiligen Einfluss des DCF-Medienzugangsverfahrens weitestgehend beseitigen.

2. IEEE 802.11 s

Der Draft IEEE 802.11s spezifiziert ein Framework für WLAN-Maschennetze und zwar für so genannte unverwaltete Maschen-Netze, z.B. kleine oder mittlere Konfigurationen, die nicht von einem Service-Provider oder einer IT-Abteilung konfiguriert und betrieben werden.

Ohne weitere Erläuterung ist klar, dass es in diesem Ansatz keine irgendwie zentrale Station gibt, die alles steuert und regelt, sondern die Maschen-Knoten sollen untereinander kommunizieren und diese Kommunikation regeln. Dabei müssen sie auch (auf dem Layer 2) Routing-Funktionen implementieren. Hier bastelt man nichts Neues, sondern verlässt sich auf zwei bestehende Verfahren von IETF: RFC 3561 „Ad Hoc On Deamnd Distance Vector (AODV) Routing“ und RFC 3626 „Optimized Link State Routing Protocol (OLSR)“.

2.1 Grundsätzliche Festlegungen

Folgende Begriffe werden zum Verständnis benötigt:

„WLAN Maschennetz“: ein WLAN Maschennetz ist ein IEEE 802.11-basiertes Wireless Distribution System (WDS), welches Bestandteil eines Distribution Systems DS ist. Es besteht aus einer Menge von zwei oder mehr Maschenpunkten, die mit 802.11 Links verbunden sind und vermöge der WLAN Maschen-Dienste miteinander kommunizieren. Ein WLAN-Maschennetz unterstützt Null oder mehr Eintrittspunkte (Maschen-Portale), automatisches Lernen der Topologie und dynamische Wegwahl, einschließlich der Wege aus mehreren Hops.

Die „WLAN-Maschen-Dienste“ regeln die Kontrolle, Verwaltung und den Betrieb des WLAN-Maschennetzes.

„Deterministische Zugriffsgelegenheit für Maschen (MDAOP)“ ist eine Zeitperiode innerhalb jedes Maschen DTIM-Intervalls, die zwischen einem Sender und einem Empfänger etabliert wird.

„Maschen Punkt (MP)“: jede 802.11 Einheit, die innerhalb einer WLAN-Masche ist und die WLAN Maschen Dienste unterstützt.

„Maschen AP (MAP)“: jeder MP, der auch AP ist.

„Maschen Portal“: ein Punkt, an dem der Übergang zu einer anderen Netztechnik, in der Regel kabelgebundenes Ethernet, erfolgt.

„Maschen Link“: eine bidirektionale 802.11 Datenverbindung zwischen zwei assoziierten Maschen Punkten.

„Link Metrik“: ein Kriterium, welches dazu benutzt wird, die Leistung, Qualität oder Wählbarkeit einer Maschen Link als Mitglied eines Maschen-Weges zu charakterisieren. Link Metrik kann für die Berechnung einer Weg Metrik benutzt werden.

„Maschen Weg“: eine Menge von verbundenen Maschen Links zwischen einem Quell-MP und einem Ziel-MP.

„Weg Metrik“: ein Kriterium für die Auswahl eines Maschen Weges.

„Maschen Topologie“: ein Graph, der die komplette Menge von Maschen Punkten und Maschen Links in einem WLAN-Maschen-Netz beschreibt.

„Maschen Nachbar“: jeder MP, der unmittelbar mit einem anderen MP durch eine Maschen Link verbunden ist.

„Maschen Unicast“: ein Frame Forwarding-Mechanismus für den Transport von MSDUs zu einem bestimmten MP innerhalb des WLAN-Maschen-Netzes.

„Maschen Multicast“: ein Frame Forwarding-Mechanismus für den Transport von MSDUs zu einer Gruppe von MPs innerhalb des WLAN-Maschen-Netzes.

„Maschen Broadcast“: ein Frame Forwarding-Mechanismus für den Transport von MSDUs zu allen MPs innerhalb des WLAN-Maschen-Netzes.

Einfache Stationen STA können keine Wege berechnen und Pakete nicht innerhalb der Masche weiterleiten. Maschen-Knoten können also mit unterschiedlichen funktionalen Leveln arbeiten. (siehe Abbildung 5)

2.2 Grundsätzliche Arbeitsweise eines WLAN-Maschennetzes

Die Entdeckung von Maschen und der Aufbau von Verbindungen zwischen gleichberechtigten Stationen erfordert, dass die Maschenpunkte genügend Informationen über sich selbst und potentielle Nachbarn haben. Dies verlangt die Entdeckung potentieller Nachbarn in der Masche durch Beacons oder aktives Scanning mittels sog. Mesh Probe Requests. Der Aufbau von Verbindungen zwischen

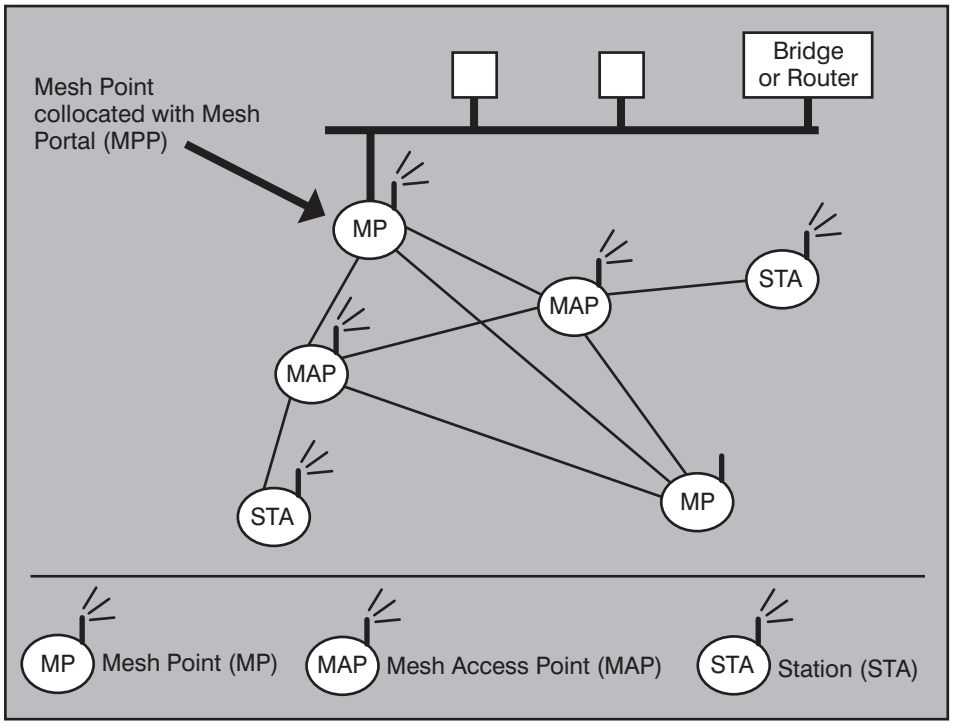


Abbildung 5: WLAN-Maschennetz mit MPs, MAPs und STAs

gleichberechtigten Knoten ist ein kontinuierlicher Prozess, der auch das permanente Monitoring von Nachbarn umfasst, um Änderungen in der Konnektivität zu erkennen und auf sie zu reagieren.

2.2.1 Die Benutzung eines Maschen Identifiers

Ein Maschen Identifier wird als eine Art Kurzbeschreibung für ein bestehendes Maschen-Netz mit bekannten Eigenschaften verwendet und von einer allseits bekannten administrativen Autorität erzeugt. Der Mesh ID kann auf vielfältige Weise in maschenfähigen Geräten installiert werden. Das liegt außerhalb der Betrachtungen des Standards. Zusätzlich kann ein Mesh ID durch den Benutzer gesetzt werden. Konzeptionell entspricht der Mesh ID einer SSID, allerdings dürfen dabei natürlich keine identischen Namen zum Einsatz kommen.

2.2.2 Entdeckung von Nachbarn

Ein Gerät muss wenigstens ein sog. Profil unterstützen. Ein Profil besteht aus einer Mesh ID, einem Path Selection Protocol Identifier und einem Path Selection Metric Identifier. Dieses Profil unterstützt die Funktion der Entdeckung von Nachbarn. Nach Definition hat ein MP mindestens ein aktives Maschenprofil.

Ein MP, der kein Mitglied irgendeiner WLAN-Masch ist, führt aktives oder passives Scanning aus, um benachbarte MPs zu finden. Im Falle des passiven Scannings kann ein Gerät nur dann als Nachbar erkannt werden, wenn genau alle der folgenden Bedingungen erfüllt sind (mit einem Probe Response Mechanismus kann man ähnliches für aktives Scanning machen):

- von dem betreffenden Gerät wird ein Beacon empfangen
- das empfangene Beacon enthält eine Mesh ID, die der Mesh ID in mindestens einem Profil des MP entspricht
- der empfangene Beacon enthält ein WLAN Maschen Capability Element mit folgenden Inhalten: eine unterstützte Versionsnummer, eine MP Aktiv Anzeige und einen Path Selection Protocol Indikator sowie einen Path Selection Metrik Indicator, der zu dem ausgewählten Profil passt

Zusätzlich sollte ein Nachbar-MP als möglicher gleichberechtigter Kommunikationspartner nur genau dann angesehen werden, wenn der Beacon ein WLAN Maschen Capability Element beinhaltet, welches einen Wert für die verfügbaren Peer Links enthält, der ungleich Null ist.

Der MP versucht auf diese Weise, alle Nachbarn und mögliche gleichberechtigte Kommunikationspartner zu finden und verwaltet die Information über die Nachbar MPs, indem er sich die MAC Adresse, die häufigsten beobachteten Link State Parameter, die empfangene Kanal-Nummer jedes in dieser Weise erkannten Gerätes gemäß den o.g. Regeln für „Nachbar“ und „Kandidat für die gleichberechtigte Kommunikation“ merkt.

Werden MP-Geräte entdeckt, müssen Mesh ID, Path Selection Protocol und Metrik Informationen in den Profilen, die ein entdeckendes Gerät hat, geprüft werden. Gibt es keine Übereinstimmung, kann das entdeckte Gerät ignoriert werden.

Ist ein MP nicht in der Lage, Nachbar-MPs zu entdecken, kann das Gerät eine Mesh-ID aus seinen Profilen nehmen und in den aktiven Zustand übergehen. Das kann z.B. geschehen, wenn ein Gerät als erstes eingeschaltet wird oder wenn mehrere Geräte gleichzeitig eingeschaltet werden.

Dies ist die Entdeckung von Nachbarn. Verbindungen zwischen ihnen werden später als Teil der kontinuierlich laufenden Prozeduren zur Maschen-Formation aufgebaut.

2.2.3 Aufbau von Verbindungen

Das Ziel des „Mesh Peer Link Establishment“ ist der Aufbau mindestens einer, meist mehrerer Verbindungen zwischen gleichberechtigten MPs. Ein MP muss in der Lage sein, mindestens eine Verbindung zu einem gleichberechtigten MP aufzubauen, er darf aber auch mehrere aufbauen und verwalten. Es ist möglich, dass es mehr gleichberechtigte MPs gibt, zu denen ein MP eine Verbindung aufbauen könnte, als der MP Verbindungen aufbauen und verwalten kann. In diesem Fall muss er sich für einige entscheiden, und zwar aufgrund statistischer Daten, die er in der Phase, als er nur in das Medium gehorcht hat, sammeln konnte, wie z.B. die Signalqualität. Die Prozeduren für Aufbau und Verwaltung von Verbindungen werden weiter unten beschrieben. Sie müssen solange für jeden möglichen gleichberechtigten MP durchgeführt werden, bis die konfigurierte Maximalzahl von MPs, zu denen ein MP Verbindungen aufbauen und unterstützen kann, erschöpft ist.

Verbindungen werden durch gleichberechtigte MPs entweder durch ein explizites Disconnect wieder abgebaut oder implizit durch ein Timeout. Die Dauer des Timeouts hängt vom Zustand der Verbindung ab. Der Zustand kann z.B. in Abhängigkeit von der Verfügbarkeit einer Mindest-Signalqualität als „Up“ oder „Down“ bezeichnet werden.

Ein MP arbeitet auf einem Grundfrequenzband. MPs, die das gleiche Grundfrequenzband benutzen, werden mittels des sog. Unified Channel Graphs zusammen dargestellt. Auf die Frequenzen und ihre unterschiedliche Benutzung sowie Gruppierungsmöglichkeiten kommen wir spä-

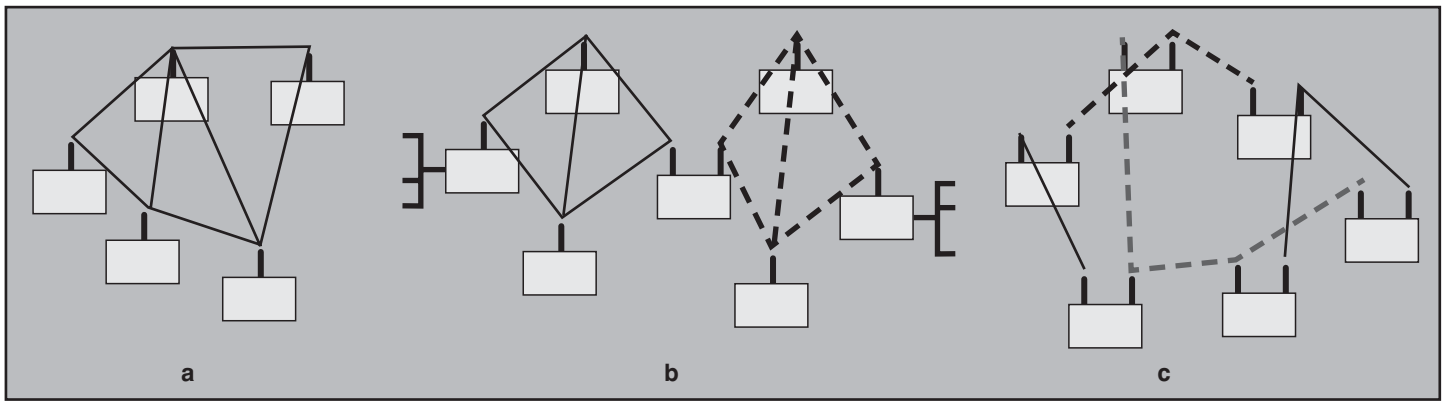


Abbildung 6: Beispiele für Kanalkonfigurationen in einem WLAN Maschennetz

ter, hier nur soviel, dass zunächst einmal nur MPs miteinander kommunizieren können, die im gleichen Frequenzband arbeiten. Ein MP muss laufend die Beacons beobachten, die von den anderen MPs, die auf dem Unified Channel Graph arbeiten, zu dem er auch gehört, gesendet werden. Wenn er einen Beacon von einem unbekannten Nachbar-MP bekommt, der aber ein passendes Match Profil enthält, muss er versuchen, zu diesem eine Verbindung aufzubauen. Aktive MPs müssen ein WLAN Mesh Capability Element in alle übertragenen Beacons und Probe Response Frames stecken. Dies hat eine bestimmte Form, die aber hier nicht weiterführt. Es enthält jedenfalls einen Status für einen aktiven MP, und die Ids des aktiven Protokolls und der aktiven Metrik. Es enthält weiterhin ein „Peer Capacity" Feld, in dem die Anzahl der gleichberechtigten Verbindungen steht, die noch unterstützt werden können.

Betrachtet man das Ganze aus der Perspektive der Verwaltungsprozeduren für Peer Links, so ist es so, dass eine Verbindung gerichtet ist, wobei ein Ende die untergeordnete und das andere die übergeordnete Station ist. Das ist mehr informativ und drückt keine Hierarchie aus. Das übergeordnete Ende entspricht der Station, die ein „Association Response" zu der Station geschickt hat, die ein „Association Request" auf den Kanal gebracht hat.

Ein MP, der eine Verbindung zu einem anderen gleichgestellten MP aufbauen möchte, schickt das „Assiciation Request", welches ein „MP peer request" Element enthält. Das unterscheidet diesen Request von einem, der von einer einfachen WLAN-Station an einen Access Point geschickt wird. Bei jedem Versuch muss eine neue Zufallszahl im sog. Richtungsfeld mitgeschickt werden. Wenn ein MP eine solche Anfrage erhält, muss er in der Tabelle seiner möglichen gleichberechtigten Partner nachschauen und zwar auf den Zustand des aktuell anfragenden MPs. Ist der Zustand „Association Pending", vergleicht er den Richtungswert mit dem, den er in seiner Tabelle vorliegen hat. Wenn der empfangene Wert kleiner oder gleich dem ist, der bereits vorliegt, muss der MP den Verbindungswunsch ablehnen und den Zustand auf „Deny" setzen. Sonst kann er den Verbindungswunsch annehmen und die entsprechende Antwort mit dem richtigen Status geben. Das Ganze ist letztlich eine einfache Methode sicherzustellen, dass ein MP, wenn er bereits mindestens eine Verbindung hat, nicht noch mal eine neue Verbindung in die gleiche Richtung aufbaut, sondern vorzugsweise in eine Richtung, die er noch nicht hat. Dadurch stellt man auf sehr einfache Weise sicher, dass die Vermaschung immer dichter wird. Da der Bereich, aus dem die Zufallszahl gewürfelt wird, endlich ist und es dann immer nach dem „größer"-Kriterium geht, iteriert der Vorgang genau dann, wenn ein MP mit seinen Nachbarn in allen Richtungen „durch" ist. Dann kann er auch eine zweite Verbindung zu einem MP aufbauen, zu dem er bereits eine Verbindung hat, wenn das Verfahren nicht anderweitig terminiert wird, z.B. durch die Anzahl der überhaupt maximal möglichen Verbindungen.

2.2.4 Messung der Verbindungsqualität

Sobald eine Verbindung zwischen benachbarten MPs aufgebaut ist, wird es notwendig, ein Qualitätsmaß zu etablieren. Das ist wichtig, damit der Path Selection Mechanismus und seine Metriken richtig funktionieren. Sobald ein Qualitätsmaß feststeht, kann die Verbindung als „Up" bezeichnet werden. Ab diesem Punkt ist der MP in der Lage, an der Wegwahl und ggf. am Forwarding teilzunehmen. Maße für die Verbindungsqualität sind wie immer Bitrate und Paketfehlerrate. Der Standard lässt aber einen weiten Bereich von Möglichkeiten, wie diese zur Festlegung eines Maßes benutzt werden können.

2.2.5 Arbeitsweise in mehreren Kanälen

Vom Standard her kann ein WLAN Maschennetz Geräte mit einem oder mehreren Radioteilen beinhalten und auf einem oder mehreren Kanälen die Kommunikation zwischen Maschenpunkten etablieren. Das sehen wir in der Abbildung 6.

Links (a) sehen wir ein einfaches Netz mit Stationen, die lediglich ein Radioteil und keine weiteren Fähigkeiten haben und deshalb auch nur einen Kanal zur Kommunikation benutzen können. In der Mitte (b) und rechts (c) sehen wir Möglich-

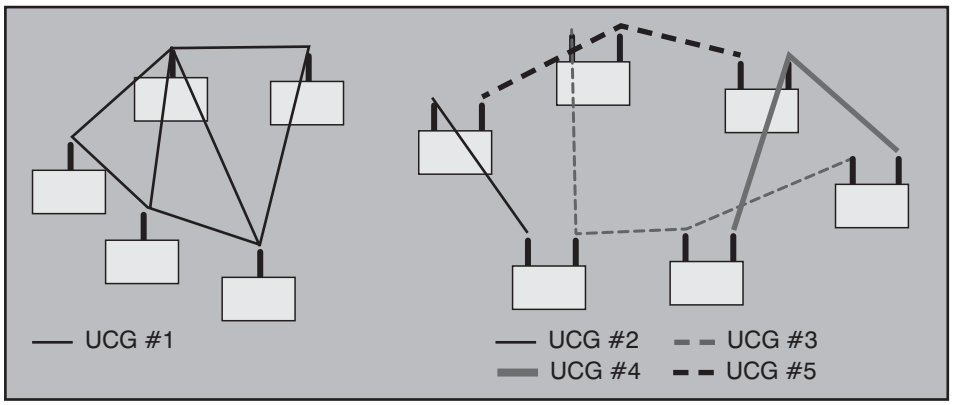


Abbildung 7: Beispiele für Unified Channel Graphs in WLAN Maschennetzen

keiten, die entstehen, wenn die Geräte besser ausgebaut sind und mehr Radioteile haben. So können mehr Kanäle benutzt werden und unterschiedliche Zuordnungsschemata von Anwendungen und Verbindungen zu Kanälen benutzt werden. Wir sehen, dass in diesen beiden Beispielen zwei oder mehr Stationen vermöge ihrer Radioschnittstellen unter Benutzung eines Kanals miteinander verbunden sind. Eine Menge von Stationen, die mittels eines Kanals verbunden sind, wird mit dem sog. Unified Channel Graph (UCG) beschrieben. Hat eine Station mehrere Radioteile und kann deshalb gleichzeitig mehrere Kanäle unterstützen, so kann sie auch mehreren UCGs angehören. Ein einfaches Netz hat nur einen UCG, während komplexere Strukturen i.d.R. mehrere UCGs haben, wie die Abbildung 7 zeigt.

Das so genannte Common Channel Framework CCF erlaubt Mehrkanalbetrieb von Geräten mit einem oder mehreren Radioteilen. Die Basis dieses Frameworks ist der sog. gemeinsame Kanal in einem UCG. Während der Benutzung von CCF wählen zwei oder mehr kommunizierende Stationen (Cluster) für eine relativ kurze Zeit einen anderen als diesen gemeinsamen Kanal und kehren anschließend in den gemeinsamen Kanal zurück. Während dieser kurzen Zeit tauschen sie einen oder mehrere DATA-Frames aus. Die Koordination für diese Kanalsprünge wird im gemeinsamen Kanal durch den Austausch von Kontroll- und Management-Frames vorgenommen. Dadurch kann man auf mehreren Kanälen gleichzeitig kommunizieren, was den Durchsatz steigert. An diesem Verfahren können durch seinen Aufbau auch Stationen teilnehmen, die zwar nur ein Radioteil besitzen, aber die Fähigkeit haben, mit diesem den Kanal zu wechseln.

Innerhalb des CCF wird der Betrieb von Stationen mit nur einem Radioteil auf unterschiedlichen Kanälen dadurch erleichtert, dass es ein so genanntes Kanal Koordinations-Fenster (CCW) gibt, welches periodisch wiederholt wird, und zwar mit der Periodendauer P. Zu Beginn jedes CCW gehen die an diesem Prozess beteiligten Stationen alle in den gemeinsamen Kanal. Während und nach dem CCW können MPs unterschiedliche Kanäle auswählen und auf diesen Übertragungen durchführen. Die Parameter P und CCW werden an alle über ein spezielles Feld des für WLAN-Maschennetze gültigen Beacon Frames kommuniziert. Das Common Channel Framework erleichtert die Kanalbildung zwischen BSS und WDS Verkehr in dem Sinne, dass ein MAP nach dem CCW in den BSS-Kanal umschalten kann und somit der MAP den „traditionellen" BSS und den „vermaschten" WDS-Verkehr handhaben kann. Außerdem kann man damit die Formation von AdHoc Clustern begünstigen.

Für die Auswahl des gemeinsamen Kanals CC müssen einige Dinge beachtet werden. Werden verschiedene Geräte gleichzeitig angeschaltet, können sie sich teilweise ggf. nicht sehen und müssen einen initialen Kanal zufällig wählen. Dadurch entsteht ein disjunktes Netz. Man braucht in diesem Falle einen kontrollierten Prozess, der es ermöglicht, dass schließlich alle Stationen mit dem gleichen Kanal arbeiten.

Vom Maschennetz als Ganzem muss erwartet werden, dass es DFS durchführen kann und somit z.B. Radarsignalen ausweicht um regulatorische Vorgaben zu erfüllen. DFS muss letztlich von allen Stationen zunächst einzeln ausgeführt werden, wie das ja schon im Standard IEEE 802.11h festgelegt ist. In manchen Netzen wird man dies durch Management-Funktionen von einem zentralen Punkt aus machen können. Generell kann man Präzedenz-Indikatoren für die Kanäle vergeben. Jeder Knoten, der nicht unter einem zentralen Management steht, wählt eine zufällige Zahl (den sog. lokalen Präzedenz-Indikator) und füllt sie in Beacons und Probe Response Nachrichten. Jeder verwaltete Knoten wählt entweder auch eine Zufallszahl oder hat bereits eine spezifische Zahl vorgegeben. Dabei dürfen sich die Zahlenbereiche von verwalteten und unverwalteten Knoten nicht überschneiden und die verwalteten müssen immer höhere Zahlen haben. Jeder Knoten merkt sich den Wert des (ihm) höchsten bekannten Präzedenzindikators im Netz und alle Knoten werden mit der Zeit den gleichen höchsten Wert erkannt haben. Dies ist dann der Präzedenzindikator für das Maschennetz und wird in Beacons von allen Maschenknoten weiterverbreitet. Treffen sich dann zwei oder mehr bislang disjunkte Maschen-Netze, ändert dasjenige mit dem niedrigeren Präzedenzindikator seinen Wert auf den höheren, und schon sind sie zusammengewachsen. Hat eine Station mehrere Radioteile, so kann sie auch unterschiedliche Präzedenzindikatoren haben und verwalten.

Fassen wir das nochmals zusammen. In einem WLAN-Maschen-Netz verständigen sich benachbarte Maschen-Knoten nachdem sie sich gefunden haben, in einem gemeinsamen Kanal. In diesem Kanal werden alle Kontrollnachrichten ausgetauscht. In einem größeren Maschennetz kann es mehrere solcher Kanäle geben, die sich ja wegen der begrenzten Reichweite der Transceiver nicht stören können, auch wenn diese logischen Kanäle auf identischen physikalischen Kanälen laufen. Durch diese Einrichtung werden verschiedene benachbarte Stationen zur Gruppen zusammengefasst. Innerhalb des Kontrollkanals läuft dann auch das recht umfangreiche Routing-Verfahren für die Path Selection innerhalb des Maschen-Netzes ab. Für die eigentliche Datenübertragung wechseln benachbarte Maschen-Punkte auf einen anderen Kanal, den sie während der Benutzung des Kontrollkanals vereinbaren. Dadurch erreicht man,

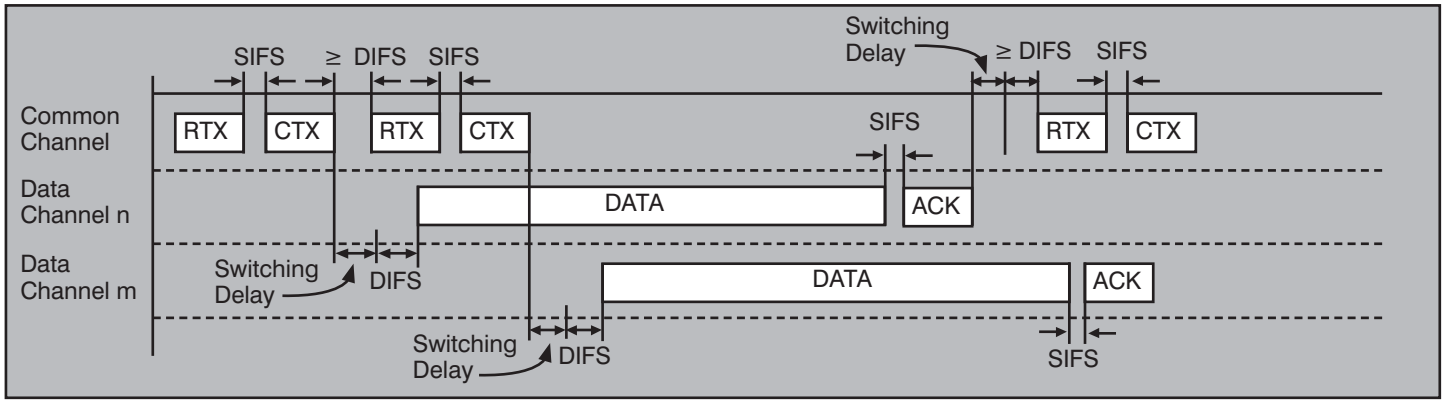


Abbildung 8: Dynamische Kanal-Auswahl

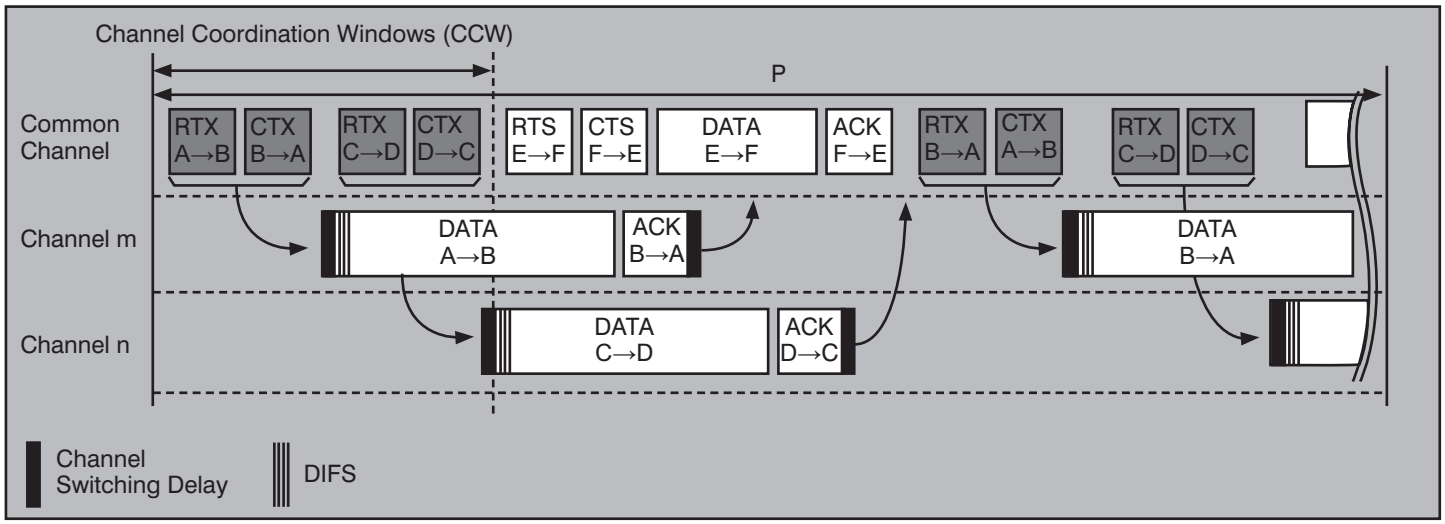


Abbildung 9: Mechanismus zur Kanal-Koordination

dass die Auswirkungen des DCF-Verfahrens, welches ja nach wie vor jeden Funkkanal hinsichtlich des wechselseitigen Zugriffs steuert, so gering wie möglich gehalten werden. In meinem zweiten Artikel zu Maschennetzen in einem späteren Insider werde ich solche Performance-Aspekte näher beleuchten. Die Abbildungen 8 und 9 zeigen nochmals die dynamische Kanal-Auswahl und den Mechanismus zur Koordination.

In 802.11s gibt es ein weiteres Verfahren, MDA Mesh Deterministic Access, welches das DCF durch ein anderes Verfahren, welches auf dem altbekannten CSMA/CA basiert, ersetzt. Leider ist es nur optional.

Schließlich sei noch erwähnt, dass es wichtig ist, Stationen, die den Maschen-Mechanismus nicht unterstützen, aber an einem Maschen Access Point assoziiert sind, besser in einem Kanal arbeiten, der weder dem gemeinsamen Kontrollkanal entspricht noch zwischen MPs für ihre Verbindungen benutzt wird. Daraus folgt unmittelbar, dass man WLAN-Maschennetze zwar theoretisch mit 11b-Transceivern im 2,4 MHz-Bereich bauen kann, besser aber auf den 5 MHz-Bereich mit 11a oder 11n und den vielen zur Verfügung stehenden Kanälen gehen sollte.

2.2.6 Path Selection und Forwarding

Die Begriffe „Mesh Path Selection“ und „Mesh Forwarding“ werden benutzt, um die Auswahl von Single- oder Multi-Hop-Wegen und das Weiterleiten von Datenpaketen über diese Wege zwischen MPs auf der Link Layer zu beschreiben. Datenpakete benutzen das übliche 802.11 Format mit vier Adressfeldern und ein wenig zusätzlicher Information, die spezifisch für ein Maschennetz ist. Client Stationen assoziieren sich üblicherweise an einem Maschen-AP wie gewöhnlich und die Menge der Maschen-APs ist logisch gesehen eine Sammlung von APs, die zum gleichen ESS gehören. Unter der Benutzung von 802.11 Management Frames (MMPDUs) werden über die Link Layer auch Nachrichten befördert, die zum Path Selection Service gehören. Ein solcher besteht aus grundsätzlichen Nachrichten für das Auffinden von Nachbarn, Messung und Wartung des Verbindungsstatus und zur Identifikation eines aktiven Protokolls zur Path Selection. In jedem WLAN Maschennetz wird nur eine einzige Methode zur Wegwahl benutzt, wenn auch ein einzelnes Gerät durchaus unterschiedliche dieser Methoden unterstützen kann.

Der Standard IEEE 802.11s gibt zwar ein spezielles Protokoll für Path Selection an, aber das ist keinesfalls ausschließlich, sondern Hersteller können auch eigene Protokolle verwenden. Deshalb gibt es ein sog. Extensible Path Selection Framework für die flexible Implementierung unterschiedlicher Protokolle und Metriken für die Path Selection. Die Spezifikation enthält ein Protokoll und eine Metrik, die immer zwingend implementiert werden müssen, um zu ermöglichen, dass Geräte unterschiedlicher Hersteller grundsätzlich miteinander kommunizieren können. Aber jeder Hersteller kann darüber hinaus auch eigene Protokolle implementieren, um z.B. bestimmte Anwendungen spezifisch zu unterstützen. Ein MP empfängt das WLAN Mesh Capability Information Element, um herauszubringen, welches Protokoll und welche Metrik in seinem Maschennetz unterstützt werden und festzustellen, ob und wie er an dem Maschennetz teilnehmen kann. Nach der Spezifikation kann ein Maschennetz, welches bereits ein anderes Verfahren als das grundsätzliche Basisverfahren benutzt, nicht von einem MP oder einer Gruppe von MPs dazu gezwungen werden, das Verfahren zu ändern, um sozusagen den kleinsten gemeinsamen Nenner zu finden.

Wir werden weiter unten die Grundzüge des Standard-Verfahrens zusammenfassen. Zunächst kümmern wir uns aber noch kurz um das Forwarding.

Wir müssen uns daran erinnern, dass Routing und Forwarding im Maschennetz reine Layer-2 Funktionen sind, weil das Netz ja nach außen hin als geschlossenes logisches Layer-2 Subnetz erscheinen soll. Wenn Datenframes in einem Multi-Hop-Maschennetz geforwardet werden, kann Multipath Routing entweder aus Gründen der Lastbalancierung oder bei dynamischen Routenänderungen leicht dazu führen, dass Frames am Zielpunkt in der falschen Reihenfolge oder doppelt ankommen. Die Wahrscheinlichkeit dafür, dass das passiert, steigt mit der Änderungsrate der Topologie, Varianzen in der Belastung und der Fluktuationsrate bei den Kanälen. Es gibt in 802.11 Headern ein Sequenzkontrollfeld. Dies wird aber nur hinsichtlich eines einzelnen Hops benutzt, um fehlende oder doppelte Frames zu erkennen und wird von jedem zwischendurch auf der Strecke liegenden MP geändert. Daher kann es für Zwecke der Ende-zu-Ende-Kontrolle nicht benutzt werden. Deshalb gibt es ein neues Feld, die Mesh E2E Sequence Number im Maschenkontrollfeld, um die von einem Quell-MP gesendeten Frames eindeutig zu identifizieren. Durch das Paar Quell-MP-Adresse und Mesh E2E Sequenz-Nummer ist ein Ziel-MP in der Lage, durcheinander gebrachte und doppelte Frames zu erkennen. Dop-

pelte Frames müssen weggeworfen und durcheinander geratene zwischengepuffert und sortiert werden, ehe sie an die LLC weitergegeben werden können. Entwicklungsziel hierbei ist natürlich eine geeignete Pufferverwaltung. Um allzu große Pufferzeiten zu vermeiden, kann ein MP auch Timer verwenden. Ist die Wartezeit erschöpft, wartet der Ziel-MP nicht länger, sondern gibt die zwischen gepufferten Pakete an die LLC ab und erklärt die fehlenden für verloren. So eine Ende-zu-Ende-Kontrolle kann nur für die Quell- und Ziel-MPs aufgesetzt werden, und es kann durchaus vorkommen, dass Pakete an Zwischenknoten ankommen, die z.Zt. außer Betrieb sind. Also, irgendwie sieht das ziemlich wackelig aus. Zum einen garantiert das Maschennetz also keineswegs die vollständige Auslieferung aller Pakete und zum anderen kann man aber die Kontrolle darüber auch nicht bis zum St. Nimmerleinstag ausdehnen, weil sonst zum einen die benötigten Rechen- und Speicherkapazitäten in jedem MP zu groß werden und zum anderen natürlich das Delay in uninteressante Bereiche vordringt. Man muss natürlich bei Funknetzen generell einen gewissen und gegenüber verkabelten Lösungen hohen Verschnitt an Datenframes hinnehmen, aber bei den bisher bekannten Lösungen wird das auf dem kurzen Wege durch schnelles Handshaking behandelt und ein fehlendes Paket kommt entweder in kürzester Zeit nach oder es gibt mit einer geringen Wahrscheinlichkeit einen Fehler. Es ist dann die Entscheidung der nachgelagerten IP-Schicht, ob sie im Interesse der Anwendung, die sie unterstützt, Pakete nachliefern lässt oder nicht. Im Maschennetz besteht aber offensichtlich kein direkter Durchgriff von Quelle zu Ziel über alle beteiligten Knoten hinweg, sondern man kann nur hoffen, dass es auf einem gewählten Weg gut geht. Wenn nicht, muss man einen neuen Weg suchen und bis zum letzten bestätigten Punkt in einer Gesamtübertragung wieder zurücksetzen. Das ist m.E. ein schwerwiegender Mangel in der Gesamtkonstruktion.

Erhält ein MP einen Unicast Datenframe mit vier Adressfeldern, so entschlüsselt er ihn und prüft auf Authentizität. Ist der Frame nicht von einer authentischen Quelle oder ist im QoS-Feld das „Untrusted“ Bit gesetzt, muss der Frame stillschweigend entsorgt werden. Danach prüft der MP, ob die Zieladresse bekannt ist. Wenn nicht, kann er den Frame wegwerfen oder zwischenspeichern und entsprechende Aktionen vom Path Selection Protokoll verlangen, z.B. indem er eine Route Error Message herausgibt. Passt die Zieladresse zu einer Station, die mit diesem MP assoziiert ist, dann wird der Frame in ein Format mit drei Adressfeldern umgewandelt und an die Zielstation geschickt. Ist die Zieladresse zwar bekannt, die Station, zu der sie gehört, aber nicht unmittelbar mit dem MP assoziiert, so wird das TTL-Feld im QoS-Feld heruntergezählt und der Frame entsorgt, wenn das Feld Null anzeigt. Sonst wird er zum nächsten Knoten weitergeschickt, die die Mesh Forwarding Table (das Ergebnis der Path Selection) anzeigt. Schickt eine assoziierte Station dem Maschen-AP einen Frame mit nur drei Adressfeldern, und sonst ist aber alles in Ordnung, macht der Maschen AP daraus einen Frame mit vier Adressfeldern und füllt in das TTL- und das QoS-Feld jeweils die Zahl 255 ein.

Erhält ein MP einen Broadcast Datenframe mit vier Adressfeldern, die mit lauter Einsen gefüllt sind, (Broadcast Adresse) so entschlüsselt er ihn und prüft auf Authentizität. Ist der Frame nicht von einer authentischen Quelle oder ist im QoS-Feld das „Untrusted“ Bit gesetzt, muss der Frame stillschweigend entsorgt werden.

Er prüft dann mittels seines lokalen Broadcast Signatur Caches, ob er diese Nachricht schon mal versendet hat. Das Tripel SA, DA und Maschen E2E Sequenznummer kann als Signatur verwendet werden. Gibt es diese schon, dann muss der Frame entsorgt werden, ist die Signatur neu, wird sie dem Signaturcache hinzugefügt. Das TTL-Feld im QoS-Feld wird heruntergezählt und der Frame entsorgt, wenn das Feld Null anzeigt. Sonst wird er zu allen Nachbarn, die am MP authentifiziert und mit ihm assoziiert sind, weitergeschickt. Ist der MP ein Maschen-AP, macht der Maschen AP aus dem Frame einen mit drei Adressfeldern und schickt ihn an die an ihm assoziierten Stationen. Mit Multicast-Frames macht er prinzipiell das Gleiche, jedoch kann er in diesem Fall ein Verfahren zur Unterdrückung von flooding benutzen, wenn es implementiert ist.

2.3 Verbindung des WLAN-Maschennetzes mit anderen Netzen

Ein WLAN-Maschennetz verbirgt die Besonderheiten seiner Funktionalität in der Schicht 2. Daher muss es für die höheren Protokolle so erscheinen, als seien alle MPs und MAPs im WLAN Maschennetz auf der Link Layer unmittelbar miteinander verbunden. Die Protokolle des Maschennetzes haben also die vornehme Aufgabe, seine eigentliche Struktur völlig zu verbergen.

Damit ein WLAN-Maschennetz als traditionelles 802-Netz erscheinen kann, muss es möglich sein, es mit anderen Netzen über Layer-2 oder Layer-3 zu verbinden. In der Abb. 10 (a) sehen wir, wie Maschennetze und traditionelle Ethernet-Segmente miteinander verbunden werden. In diesem Fall arbeitet jeder MP, der die Funktion Mesh Portal (MPP) beherrscht, als Bridge mit einem Standard-Brückenprotokoll wie IEEE 802.1D. Die Abbildung 10 (b) wiederum zeigt die Zusammenschaltung von gemischt traditionellen Ethernets und Maschen WLANs über einen IP-Router. In diesem Fall müssen die MPPs auch die IP Gateway Funktion unterstützen. So entsteht ein Netz mit zusammen geschalte-

WLAN Maschen-Netze ante portas!

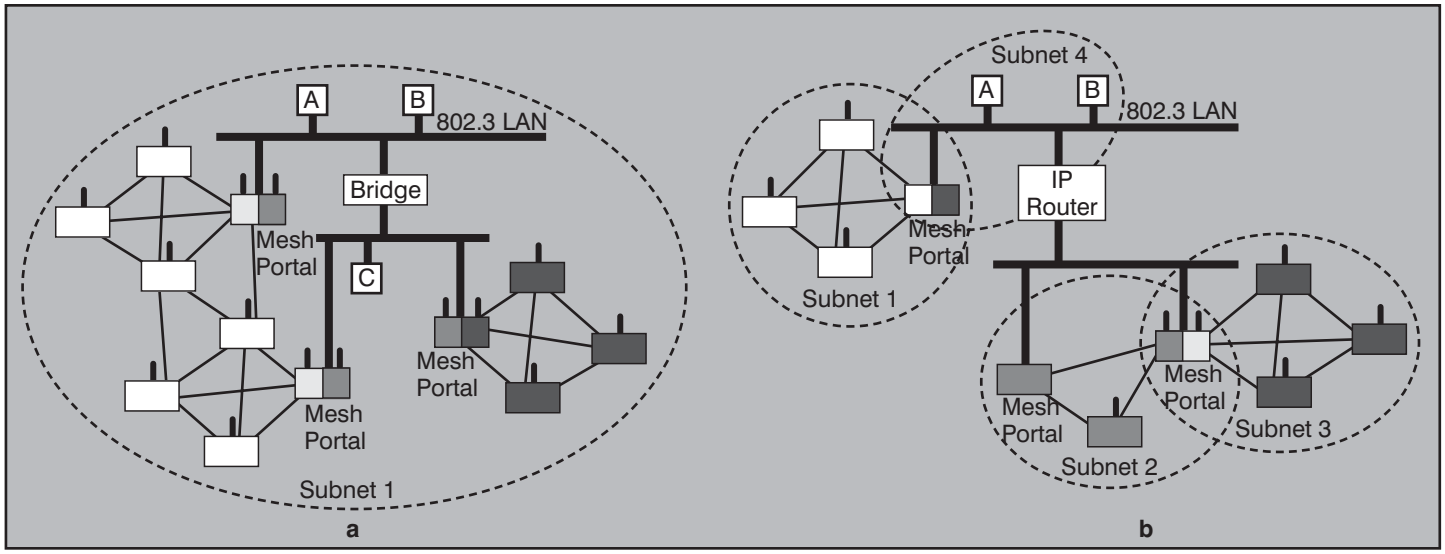


Abbildung 10: Verbindung des WLAN-Maschennetzes mit anderen Netzen

ten Layer-2-Subnetzen, die ihrerseits wieder aus Segmenten und WLAN-Maschen bestehen.

Schließlich können WLAN-Maschen-Netze auch über Mesh Portals MPs untereinander zusammengeschaltet werden, wenn sie z.B. unterschiedliche Layer-3-Protokolle unterstützen oder unterschiedlich konfiguriert sind.

Dadurch entsteht das Referenzmodell für Internetworking von WLAN-Maschen-Netzen, wie es in Abbildung 11 zu sehen ist. Wie man sieht, erscheint die WLAN Maschen MAC Arbeitseinheit einem 802.1 Relay oder einem L3-Router als einzelner Port. Das Maschennetz erscheint als einzelnes, schleifenfreies LAN-Broadcast Segment.

Das MAC-Frameformat sieht relativ bekannt aus, auffällig ist lediglich das Feld für Mesh Forwarding Control. Die maximale MSDU-Länge ist 2304 Oktette zuzüglich ggf. Overhead durch Security Encapsulation. (siehe Abbildung 12)

Die Interaktion zwischen dem Path Selection Verfahren im WLAN-Maschennetz und einem Layer-2-Bridging geschieht an zwei Stellen: an jedem MP, der einem Maschen-Portal MPP zugeordnet ist und auf jedem Knoten im WLAN-Maschennetz. Ein Paket, was von einem MP, der einem MPP zugeordnet ist, gesendet oder geforwardet wird, hat drei mögliche Ziele:

- einen Knoten im Maschennetz
- einen Knoten außerhalb der Masche, der erreicht werden kann, ohne das Maschennetz zu durchlaufen
- einen Knoten außerhalb des Maschennetzes, der durch das Maschennetz erreicht werden kann.

Ein Paket, welches von einem Knoten innerhalb des WLAN-Maschennetzes gesendet wird, hat zwei mögliche Ziele:

- einen Knoten innerhalb des Maschennetzes
- einen Knoten außerhalb des Maschennetzes

Der Standard setzt voraus, dass jeder Knoten im Maschennetz, der einem MPP zugeordnet ist, an transparentem Layer-2 Bridging teilnehmen kann. So kann jeder MP, der einem MPP zugeordnet ist, am Spanning Tree Protokoll teilnehmen und eine Knotentabelle verwalten, an der er sehen kann, durch welchen Port jeder Knoten im logischen Netzwerk erreicht werden kann. Im Standard werden auch verschiedene relativ harmlose Erweiterungen beschrieben, mit denen es möglich ist, dass ein MP, der einem MPP zugeordnet ist,

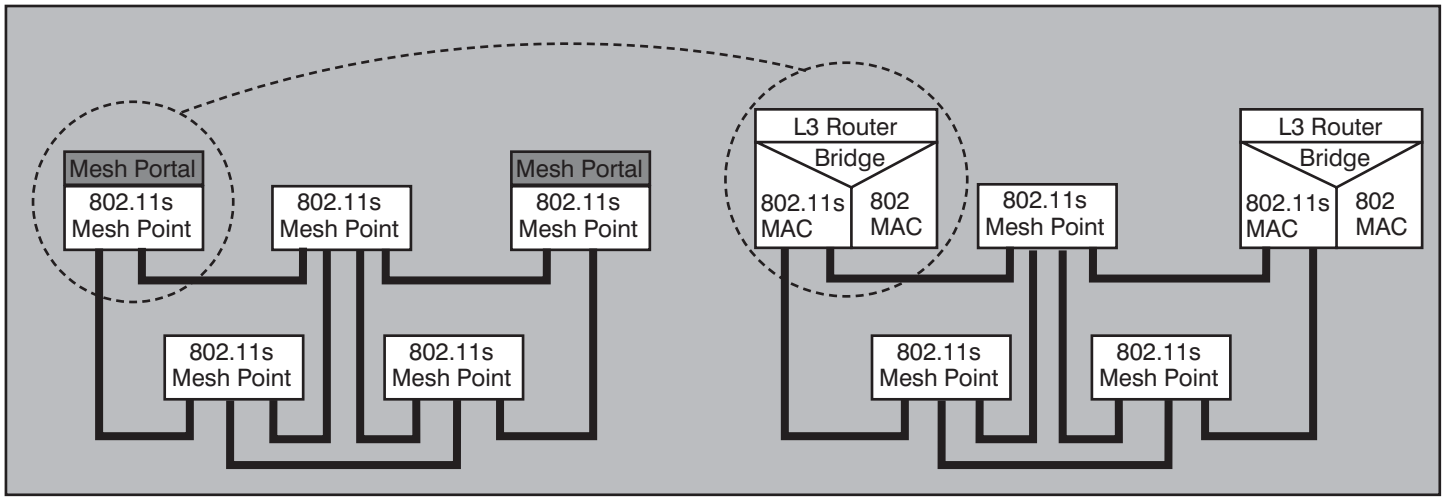
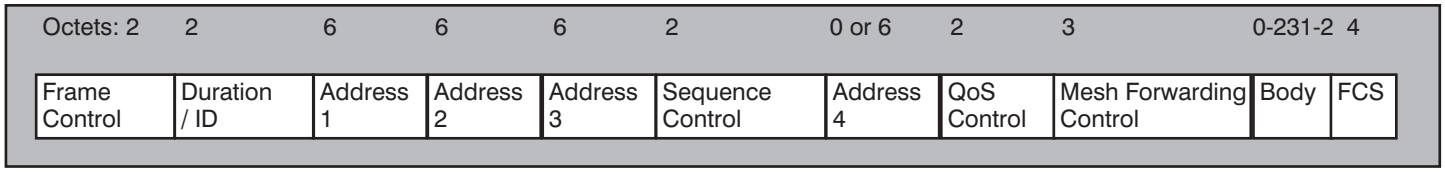


Abbildung 11: Referenzmodell für WLAN-Maschen-Netz-Internetworking



Octets: 2	2	6	6	6	2	0 or 6	2	3	0-231-2	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	Mesh Forwarding Control	Body	FCS

Abbildung 12: MAC Frame Format

auch als transparente Layer-2-Brücke fungieren kann. Das führt hier an dieser Stelle hinsichtlich des Gesamtverständnisses aber nicht wesentlich weiter.

Abschließend sein noch bemerkt, dass von der Konstruktion eines WLAN-Maschennetzes nach IEEE 802.11s auch verlangt wird, dass es die Standards IEEE 802.1 D, Q und F unterstützt und somit auch die Bildung von VLANs.

2.4 Metrik und Path Selection

Um Kompatibilität zwischen Geräten unterschiedlicher Hersteller sicherzustellen, gibt es eine default Metrik und ein default Path Selection Verfahren. Jeder Hersteller kann jedoch zusätzlich weitere Verfahren implementieren, allerdings auf Kosten der Interoperabilität.

2.4.1 Metrik

Um aus der von jedem Knoten generierten Link State Information eine Unicast Forwarding Tafel berechnen zu können, muss der MP zunächst für jede paarweise Verbindung im Maschennetz die Kosten berechnen. Es gibt im Standard einen Vorschlag für eine Metrik, die als default angesehen werden kann, andere Metriken sind natürlich immer möglich, weil die default Metrik immer durch das Erweiterbarkeits-Framework überschrieben werden kann. Die Kostenfunktion für den Aufbau von Wegen mit Funkübertragung basiert auf sog. Airtime Costs, also Kosten, die sich an der Benutzungsdauer des Übertragungsmediums orientieren. Das Maß ist approximativ. Es ist die Summe aus dem Overhead für den Kanalzugriff, dem Protokolloverhead und der Anzahl der Bits in einem Testframe geteilt durch die Rate, mit der man den Testframe unter den aktuellen Umständen senden könnte multipliziert mit dem Reziprok von 1 abzüglich der aktuellen Bitfehlerrate. Ein griffiges Maß. Hier wird darauf Rücksicht genommen, dass es innerhalb eines Maschennetzes Radioverbindungen unterschiedlicher Norm zwischen den Knoten geben kann. So ist eine 11b-Verbindung, die schon in den ersten beiden Summanden eine Verzögerung von fast 700 μsek hat, unter den gleichen Randbedingungen deutlich „teurer“ als eine Verbindung mit 11a, die es in diesen Summanden lediglich auf 185 μsec. bringt. Mit einer solchen Metrik wird erzielt, dass das Maschennetz die schnellen Routen bevorzugt, was ja auch sinnvoll ist.

2.4.2 Path Selection mit dem Hybrid Wireless Mesh Protocol HWMP

HWMP ist ein Wegwahlverfahren, welches nach Angaben seiner Erzeuger die Flexibilität von bedarfsgesteuerter Routenermittlung mit Erweiterungen für das effiziente proaktive Routing, welches im Zusammenhang mit Mesh Portals gebraucht wird, kombiniert. Die hybride Natur erlaubt die flexible Wegwahl sowohl in infrastrukturellen als auch in ad Hoc Maschen-Netzen. Die Kombination von On-demand und proaktivem Routing erlaubt es, dass die MPs entweder selbst optimale Routen entdecken und verwalten oder Informationen dafür nutzen, die von einem Root-Knoten im Zusammenhang mit einer Baumstruktur erzeugt und weitergegeben werden. In beiden Fällen geschieht die Auswahl von geeigneten Nachbarknoten auf dem Weg nach einer Metrik. HWMP benutzt eine einzelne Menge von Protokollprimitiven und Verarbeitungsregeln aus dem „Ad Hoc On-Demand Distance Vector“ AODV-Protokoll (IETF RFC 3561) für alle Funktionen, die mit dem Routing zusammenhängen. Die weiter unten beschriebenen Verarbeitungsregeln sind immer dann in Kraft, wenn das default Path Selection Protokoll aktiv ist.

Besitzt ein Maschen-Netz keinen Root-Knoten, so wird für die gesamte Wegwahl on-demand Routing verwendet. Gibt es einen konfigurierten Root-Knoten, kann dieser dazu benutzt werden, einen möglichen Weg zum Root Knoten zu bestimmen. Die Einrichtung von Routen entlang des Baumes wird mittels sog. Request und Reply Regeln verwaltet. Ein baumstrukturiertes Netz wird dadurch vorbereitet, dass man einen MP, üblicherweise ein Mesh Portal, als Root konfiguriert. In diesem Falle werden andere Maschenknoten die Wege zum Root-Knoten proaktiv verwalten und es wird ein proaktiver Routing Baum auf der Basis von Distanzvektoren aufgebaut und gepflegt. Jeder Knoten kann darüber hinaus Wege zu anderen Knoten aufbauen, indem er die normalen AODV Verarbeitungsregeln und Primitive benutzt.

HWMP ermöglicht einen einfachen hybriden Setup für einen Weg. Wenn ein proaktiver Baum existiert, wird dieser per Default benutzt während das on-demand Route Discovery noch läuft. HWMP erlaubt einem Knoten im Maschen-Netz den Aufbau einer Route zum Root-Knoten unter Benutzung des proaktiven Routing-Trees. Der Knoten darf aber gleichzeitig Management-Frames bearbeiten, die von einem anderen MP des WLAN-Maschennetz im Zuge seines Versuchs, on-demand Routing durchzuführen, ausgesandt wurden.

Insgesamt ergeben sich nach IEEE 802.11s folgende Vorzüge des Verfahrens: es kann für einen weiten Bereich von Anwendungsszenarien eingesetzt werden und funktioniert sogar für mobile Maschen-Netze. Die MPs finden aufgrund der Metrik den bestmöglichen Weg in einem Maschennetz. Gibt es einen Root-Knoten, treten weitere Vorzüge hinzu: ist das Ziel außerhalb des Maschen-Netzes, so wird eine Überflutung desselben durch entsprechende (erfolglose) Route Discovery Pakete vermieden. Die Notwendigkeit, Pakete an der Quelle während eines laufenden Route-Discovery Prozesses zwischenzuspeichern, wird deutlich reduziert. Broadcast-Verkehr, der nicht zur Route Discovery gehört, kann entlang der Baumtopologie ausgeliefert werden. Gibt es Änderungen oder Schwierigkeiten im Rahmen der Topologie oder mit der Verfügbarkeit der Root oder des Baumes, kommt man mit on-demand Routing nicht nur operativ weiter, sondern kann dem Baum helfen, wieder auf die Beine zu kommen, um es einmal einfach auszudrücken.

2.4.2.1 On-demand Routing in HWMP

On-demand Routing in HWMP benutzt einen Route Requenst (RREQ) und einen Route Reply (RREP)-Mechanismus zum Aufbau von Verbindungen zwischen zwei Knoten. Jeder Knoten bestimmt die Kosten für die Verbindung zu seinen Nachbarn nach der oben beschriebenen Metrik. Um die metrischen Informationen an die anderen Knoten weiterzugeben, gibt es spezielle Felder in den RREQ- und RREP-Nachrichten. Möchte ein Knoten S eine Route zu einem Ziel D finden, schickt er ein Broadcast mit RREQ und D als Zielparameter. Der metrische Parameter wird dabei auf 0 gesetzt. Jeder Knoten kann von diesem RREQ von S mehrere Kopien erhalten. Jeder RREQ durchläuft einen einzigartigen Weg von S zu einem emp-

fangenden Knoten. Empfängt ein Knoten ein RREQ, bestimmt er eine Route nach S oder macht ein Update auf eine bestehende Route, wenn der RREQ noch frisch genug ist und durch eine Route traversiert wurde, die hinsichtlich der Metrik besser ist als die bisher bekannte. Wird eine Route neu kreiert oder upgedatet, so wird das RREQ wiederum gebroadcastet. Wann immer ein Knoten ein RREQ weiterleitet, muss das metrische Feld im RREQ upgedatet werden, um die kumulative Metrik der Route zur Quelle des RREQs aus der Perspektive des weiterleitenden Knotens widerzuspiegeln. Erreicht dieser Prozess das gewünschte Ziel D, so sendet D ein RREP als Unicast an S. Zwischenknoten erzeugen üblicherweise keine RREPs, auch wenn sie den Weg zu D eigentlich kennen, es sei denn, das „Destination Only“ Flag steht auf Null. Default ist es immer auf 1, damit nur das Ziel ein RREP sendet. Ist das Flag auf Null und kennt der Zwichenknoten den Rest des Weges zu D, schickt er ein Unicast RREP an S. Auch gibt es ein „Reply and Forward“ Flag, mit dem beide Mechanismen kombiniert werden können. Ziel ist es, dass ein Knoten von den bei den Zwischenknoten bereits vorliegenden Informationen profitieren kann und man das Delay für die Wegwahl und Zwischenpufferung auf diese Weise deutlich reduziert, ohne dass man darauf verzichten muss, eine Route mit der bestmöglichen Metrik zu wählen. Dadurch gibt es noch verschiedene Varianten, die wir hier aber nicht weiter diskutieren können. Irgendwie erinnert das On-Demand Routing an eine stark verbesserte und optimierte sowie mit einer Metrik versehene jüngere Schwester des Source Routings aus dem Token Ring selig.

Es gibt noch einige optionale Erweiterungen des Grundverfahrens. Zum einen ist es so, dass Routen mit der Zeit ja „schlecht“ werden können, z.B. wenn sich die Topologie oder die Randbedingungen wesentlich ändern. Um nicht in jedem Falle alles neu berechnen zu müssen, gibt es eine periodische Routenauffrischung. Bei dieser wird ein RREQ gesendet, ohne dass ein konkreter Grund in Form einer anstehenden Übertragung vorliegt. So können Routen immer mit einer guten Metrik frischgehalten werden. Zum anderen kann es passieren, dass eine Übertragung ansteht, während man grade dabei ist, die Routen aufzufrischen. Dann muss eigentlich noch mit der alten bekannten Route gearbeitet werden, auch wenn diese eben nicht mehr besonders frisch ist, es sei denn, es wird eine weitere Option implementiert, die das sofortige Umschalten auf eine neue Route auch während einer aktuellen Übertragung erlaubt. Diese Option ist natürlich auch dann besonders nützlich, wenn ein Knoten vorübergehend ausfällt. In diesem Fall müssen ja Routen mit Umgehungswegen benutzt werden, die natürlich eine schlechtere Metrik haben. Ist der Knoten dann wieder aktiv und hat sich nach den bislang beschriebenen Verfahren (Finden von Nachbarn usf.) wieder in das Maschen-Netz eingegliedert, ist es sinnvoll, ihn auch wieder zu benutzen, wenn er auf dem Weg liegt und die Umleitungen zu deaktivieren.

2.4.2.2 Baum-basiertes Routing in HWMP

Wird ein Maschen-Punkt (üblicherweise ein Maschen Portal) in einem WLAN-Maschennetz optional als Root konfiguriert, können andere Knoten ihre Routen zu diesem Konten proaktiv erstellen und verwalten, indem sie die RREQ und RREP Prozeduren und Primitive zum Aufbau von Routen zu diesem Knoten einsetzen.

Ist HWMP das aktive Protokoll und wurde ein Root-Knoten konfiguriert, beginnt die Formation der Topologie dadurch, dass der Root Knoten sich mit der route announcement Nachricht vorstellt, die die Distanz Metrik und eine Sequenznummer beinhaltet. Der Wert der Metrik wird auf Null initialisiert. Jeder MP, der das Route Announcement hört, berechnet unter Benutzung der weiter unten erklärten Primitive zur Routenetablierung eine Route zum Root Knoten. Wenn die Prozedur zum Aufbau einer Route funktioniert, macht der MP direkt ein Update seiner Routing-Tafel und identifiziert sich selbst als direkt mit der Root verbundenes „Kind“. Der MP bringt auch die mit der Route assoziierte Metrik auf einen neuen Stand. Der MP muss das Route announcement mit der aktualisierten Metrik rebroadcasten. So baut sich die Topologie vom Root Knoten her auf, indem jeder MP den Distanz-Vektor zur Root undatet und zusätzlich all seinen Nachbarn die kumulativen Kosten zum Root Portal mitteilt.

Root Announcements sind Broadcasts, die der Root Knoten periodisch mit steigenden Sequenznummern aussendet. Das HWMP-Registrations-Flag differenziert des Weiteren zwischen einem unidirektionalen Baum von allen MPs zum Root Knoten und einem vollständigen Baum, in dem die MPs sich beim Root Knoten registrieren, um Wege vom Root Portal zu allen MPs zu bestimmen. Ist das HWMP-Registrations Flag im Route Announcement nicht gesetzt, gibt es keine weitere Bearbeitung der Route Announcement Nachricht auf einem individuellen MP außer der Weiterleitung der Nachricht zu seinen Nachbarn. Ist das Flag gesetzt, speichert der MP die Nachricht und wartet eine bestimmte Zeit, ob andere derartige Nachrichten ankommen. Ist die Zeit um, kann der MP ein RREQ broadcasten, in dem das TTL-Feld auf 1 steht und das die Zieladresse der Root enthält, die er aus dem Root Announcement gelernt hat. Jeder Nachbar, der nur einen Hop entfernt ist, kann mit einem RREP antworten, der die aktuellste verfügbare Metrik für die Verbindung zum Root Knoten enthält. Ein MP, der diese Nachricht erhält, muss sich

das Elternteil (Root-Knoten) mit der günstigsten Metrik aussuchen. Ein MP kann den RREQ mehrfach rebroadcasten.

Hört ein MP keine Root Announcement Nachricht in einer vordefinierten Zeitspanne oder erhält er keinen sinnvollen Path zur Root aus den RREQs, kann er nicht am Aufbau des Baumes teilnehmen bis er ein gültiges Root Announcement hört.

Sobald ein MP einen Eltern-MP für seinen Weg zur Root aussucht, pflegt er diesen durch periodisches Senden eines Wartungs-RREQ an das Elternteil und den Empfang eines entsprechenden RREPs. Er kann auch periodisch Broadcasts mit Topologie-RREQs aussenden, um immer sicher zu sein, dass er den Weg mit der besten Metrik zur Root benutzt. Aus Optimierungsgründen darf er das aber nicht zu oft machen und deutlich seltener als das Wartungs-RREQ. Wenn das Elternteil nicht in der Lage ist, den Weg mit der günstigsten Metrik zur Root anzubieten, dann darf sich der MP ein neues Elternteil mit einer besseren Metrik nach Regeln, die im Root Knoten festgelegt sind, suchen. Geht der aktuelle Pfad verloren, sendet der MP sofort ein Topologie-RREQ als Broadcast gefolgt von einem RRER die Topologie herunter, damit jeder Knoten mit on-demand-Routing, der diesen Weg noch in der Tabelle hat, den betreffenden Eintrag löschen kann. Der gleiche RRER wird den Baum heraufgeschickt, wenn man ein anderes Elternteil gefunden hat. Wege in der Topologie benötigen kein weiteres Update, bis das Finden eines anderen Elternteils fehlschlägt. Kann innerhalb eines bestimmten Intervalls kein anderes Elternteil gefunden werden, wird ein RRER an alle Kinder geschickt.

Falls das HWMP Reguistrations Flag in der Root Announcement Message gesetzt war, wenn ein MP einen Eltern-MP für seinen Weg zur Root auswählt, registriert er sich selbst an der Root, indem er ein sog. Gratuituos RREP mit seiner eigenen Adresse und den Adressen aller an ihm assoziierten Stationen ohne Maschen-Fähigkeit sendet. Jeder MP, der auf dem Weg liegt und diese Nachricht sieht, updatet die Routing Tafel hinsichtlich des MPs, von dem die Nachricht ausging und beschreibt ihn als „Next Hop-Kind“, wobei er aber nicht gezwungen ist, sich auch die Adressen aller assoziierten Stationen ohne Maschenfähigkeit zu merken. Wenn MPs das Elternteil wechseln müssen, z.B. weil sie dazu durch einen Ausfall einer Verbindung gezwungen werden, senden sie immer ein Gratuituos RREP zum Root Knoten, um die dazwischenliegenden MPs zum Update zu veranlassen. Als Reaktion gibt der Root Knoten ein RRER für den alten, nicht mehr benutzten Weg.

Möchte ein Knoten einen Frame an einen anderen Knoten schicken, und hat keinen Weg, der zu diesem Knoten führt in seinen Tafeln, kann er den Frame auch an den Root-Knoten schicken. Der Root sieht nach, ob die Pakete für einen Knoten im WLAN-Maschennetz oder für ein Ziel außerhalb des Maschennetzes bestimmt ist. Findet auch der Root Knoten keinen passenden Eintrag in seinen Routing Tafeln, so schickt er das Paket über sein Uplink weg. Das ist ein wichtiger Grund dafür, warum es günstig ist, wenn man ein Maschen-Portal zum Root Knoten macht, weil ein Knoten, der keine Portal-Fähigkeit und damit kein Uplink hat, diese wichtige Funktion leider nicht ausführen kann. Der Root Knoten ist insgesamt dafür verantwortlich, zu entscheiden, ob ein Ziel innerhalb oder außerhalb des Maschennetzes ist. Falls notwendig, muss er ein RREQ los senden, um die Routen-Suche zu starten. Findet er auf diese Weise das Ziel, schickt er den Frame zum Eltern-Knoten des Ziel-MP und versieht sie mit einem speziellen TA. Erreicht das Paket den Eltern MP und er sieht diese spezielle Markierung, weiß er, dass der ursprüngliche Absender nicht der Root Knoten, sondern ein anderer MP innerhalb des Maschen-Netzes ist. Also initiiert er ein RREQ zurück zur ursprünglichen Quelle. Dieser hybride Routing-Mechanismus erlaubt es, dass der initiale Frame über die bestehende Baumtopologie (zur Root) geschickt wird und danach eine on-demand Route zwischen den eigentlich kommunizierenden MPs aufgesetzt wird. Jeder Frame, der vom Root Knoten ausgesendet wird, folgt dem hinsichtlich der Metrik optimalen Pfad zu jedem anderen Knoten im Maschen-Netz.

Gibt es in einem WLAN Maschen-Netz mehrere Maschen Portale, sollte ein einzelnes Portal die Rolle des Root-Knotens übernehmen, entweder indem man es direkt so einrichtet oder durch eine dynamische Prozedur. In diesem Fall nehmen alle anderen Portale keine Root-Funktionalität an. Gibt es mehrere Maschen-Portale, forwardet die Root alle Pakete mit unbekanntem Ziel sowohl über ihr eigenes Uplink als auch über alle Uplinks der anderen Portale. Alle Portale, die nicht Root sind, forwarden alle Frames, die von ihren Uplinks kommen, zum Root Portal zur Weiterverarbeitung. Sollten mehrere Portale an das gleiche LAN-Segment angeschlossen sein, kann ein externer STP, der im LAN-Segment läuft, den Uplink eines Portals blockieren, wie er das auch bei anderen Teilnetzen macht.

Es gibt noch viele weitere Einzelheiten zu diesem Path Selection Protokoll, deren Diskussion hier aber nicht wesentlich weiterführt. Die Stärke des Protokolls liegt darin, dass durch die Mischung von on-demand und Tree-basiertem Routing eine hohe Dynamik der Topologie unterstützt wird und vor allem das Wegnehmen oder Einfügen neuer MPs überhaupt keine Probleme machen sollte. Dadurch, dass alle Routing-Nachrichten auf dem Kontrollka-

nal abgehandelt werden und somit von der eigentlichen Datenübertragung getrennt sind, sind wirklich negative Auswirkungen durch die Tatsache, dass der Kontrollkanal wie alle 802.11 WLAN-Medien durch das alte DCF-Verfahren gesteuert wird, eigentlich nicht zu befürchten. Wir werden solche Themen aber noch in einem weiteren Artikel aufgreifen.

Die verwendete Metrik ist sinnvoll, allerdings muss man feststellen, dass sie bei einem Mix unterschiedlicher Technologien, also 802.11 b,a,g,h oder n immer die schnelleren Zellen bevorzugt. Grade das ist aber auch besonders sinnvoll, weil das Forwarding durch langsamere Zellen ja ein Paket erheblich aufhalten würde.

Im Standard wird optional noch ein weiteres Routing Protokoll beschrieben, das sog. Radio Aware Optimal Link State Routing Protokoll RA-OLSR. Es basiert auf dem im RFC 3626 beschriebenen OLSR mit Erweiterungen vom sog. Fisheye State Routing FSR und der Benutzung von Metriken, die sich ebenfalls des Radio-Umfeldes bewusst sind. Um den Kontroll-Overhead zu minimieren, werden nicht alle Kontroll-Informationen an alle Knoten gebroadcastet, sondern nur an bestimmte, die einer Untermenge angehören und als Multipoint Relays bezeichnet werden.

3. Ausblick und Konsequenzen für die Unternehmensnetze

WLAN-Maschen-Netze nach IEEE 802.11s bieten ein riesiges Gestaltungspotenzial. Dies gilt für den Konsumer- und den Enterprise-Markt. Ihre Flexibilität, der mit ihnen verbundene Zugewinn an Verfügbarkeit und Kapazität, aber auch ihre Portabilität eröffnen ein weites Spektrum an Nutzungsmöglichkeiten. Gerade mit dieser Technologie wird deutlich, wie weit funkgebundene Netze den kabelgebundenen überlegen sein können.

Theoretisch müssten die heute verfügbaren Access-Points mit Mehr-Radio-Technik - insbesondere wenn sie schon WDS unterstützen - auch in der Lage sein, den IEEE 802.11s-Standard sofort umzusetzen. Fragezeichen mögen hinter der notwendigen CPU-Leistung stehen. Mit der Einführung von IEEE 802.11n kommen aber auf Grund der dann notwendigen Gigabit-Unterstützung sowieso sehr leistungsstarke CPU´s zum Einsatz. Spätestens damit wird sich die Tür in die neue Maschenwelt öffnen.

Bisher ist IEEE 802.11s noch Draft und die Erfahrung mit diesen Technologien hat gezeigt, dass man den Praxiseinsatz abwarten muss, bevor ein endgültiges Urteil möglich ist. Hersteller können natürlich neben den durch den Standard vorgegebenen Verfahren für Path Selection und Forwarding eigene Verfahren implementieren, vor allem dann, wenn sie damit Erfahrung haben. Dies dürfte auf alle etablierten Netzkomponenten-Hersteller zutreffen, aber speziell Cisco kann hier auf etliche bestehende Verfahren zurückgreifen.

Auch für den Konsumer-Bereich könnte es schnell Produkte geben, um eine Versorgung eines Hauses mit mehreren Access-Points ohne Kabelverbindung zu ermöglichen (durchaus interessant für größere Mietgebäude).

Man muss abwarten, ob Maschennetze auch mit beweglichen Knoten und sich schnell ändernden Routen klar kommen. Damit würden sich weitere Einsatzfelder eröffnen.

IEEE 802.11s schreibt im Draft, dass die Lösung vorzugsweise für kleine und mittlere Installationen gedacht ist. Abgesehen davon, dass sehr viele Installationen genau in diesen Bereich fallen, gibt es keinen wirklichen Grund, warum das Konzept nicht auch auf die Perspektive größerer Bereiche ausgedehnt werden kann, was aber wirklich maßgeblich von der Konstruktion und Leistung der MP-Prozessoren abhängt.

Insgesamt kann man sagen: die WLAN-Maschen-Netze stehen unmittelbar vor der Tür. Lassen wir sie herein!

Report des Monats

Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

Sie erhalten mit diesem Report ein umfassendes Grundlagenwerk, das Sie bei der Auswahl und beim Aufbau einer 802.1X-basierende Sicherheitslösung unterstützt, auf die verborgenen Fallstricke dieses Frameworks aufmerksam macht und wesentliche Betriebsaspekte offen legt.

Im Folgenden stellen wir Ihnen einen Auszug als Leseprobe zur Verfügung:

1.1 Auswahl der Authentifizierungsmethoden

Bei der Wahl der EAP-Methode(n) sind im Wesentlichen die folgenden Punkte zu beachten:

- Welche Clients sollen unterstützt werden?
  - Geräte- oder Benutzerauthentifizierung?
- In welche Betriebssystem-Landschaft soll die Lösung integriert werden?
- Steht eine PKI zur Verfügung oder soll eine aufgebaut werden?
  - Falls Ja, sollen/können die Clients mit Zertifikaten ausgestattet werden oder nur die Authentifizierungsserver?
  - Falls alle oder auch nur einige Clients keine Zertifikate erhalten, gegen welche Datenbasis soll dann authentifiziert werden?
- Soll die Anbindung von Clients über Wireless LAN unterstützt werden?

1.1.1 Geräte- oder Benutzerauthentifizierung

Die in Kapitel 3 vorgestellten Standards unterscheiden nicht zwischen Geräte- und Benutzerauthentifizierung. Tatsächlich ist diese Unterscheidung auch etwas akademisch, die beiden Begriffe stammen ursprünglich aus der Windows-Welt, wo im Active Directory Benutzerkonten und Computerkonten geführt werden. Eine Authentifizierung kann hier folglich gegen ein Benutzerkonto (= Benutzerauthentifizierung) oder gegen ein Computerkonto (= Geräteauthentifizierung) erfolgen.

Der entscheidende Unterschied zwischen beiden Authentifizierungstypen ist also nicht die Frage, welcher Kontentyp genutzt wird, sondern: Erfolgt die Authentifizierung mit oder ohne Interaktion mit einem Benutzer?

Unter Geräteauthentifizierung versteht man also einen Authentifizierungsvorgang, der ohne Eingaben von Benutzerseite automatisiert abläuft. In diesem Fall müssen die benötigten Authentifizierungsdaten (Credentials) folglich auf dem System lokal vorliegen.

Hiermit stellt sich unmittelbar die Frage nach der Sicherheit

1. für die hinterlegten Credentials auf dem Gerät und
2. für das zu schützende Netzwerk.

Bei Benutzerauthentifizierungen setzt man meist auf die Komponente „Wissen“ (in der Regel ein Passwort) oder auf eine Kombination aus den Komponenten „Wissen“ und „Besitz“ (z.B. Smartcard plus PIN), anhand derer der Benutzer identifiziert wird. Beides geht bei der Geräteauthentifizierung natürlich nicht, das Gerät identifiziert sich eben allein, Passwort oder Zertifikat sind direkt auf dem Gerät hinterlegt. Daher muss sichergestellt werden, dass diese Daten (Credentials) nicht entwendet und von anderen Systemen für einen unberechtigten Netzzugang missbraucht werden können.

Von den in Kapitel 3 vorgestellten EAP-Methoden nutzen die meisten ein Passwort zur Clientauthentifizierung und benötigen daher die Interaktion mit einem Benutzer

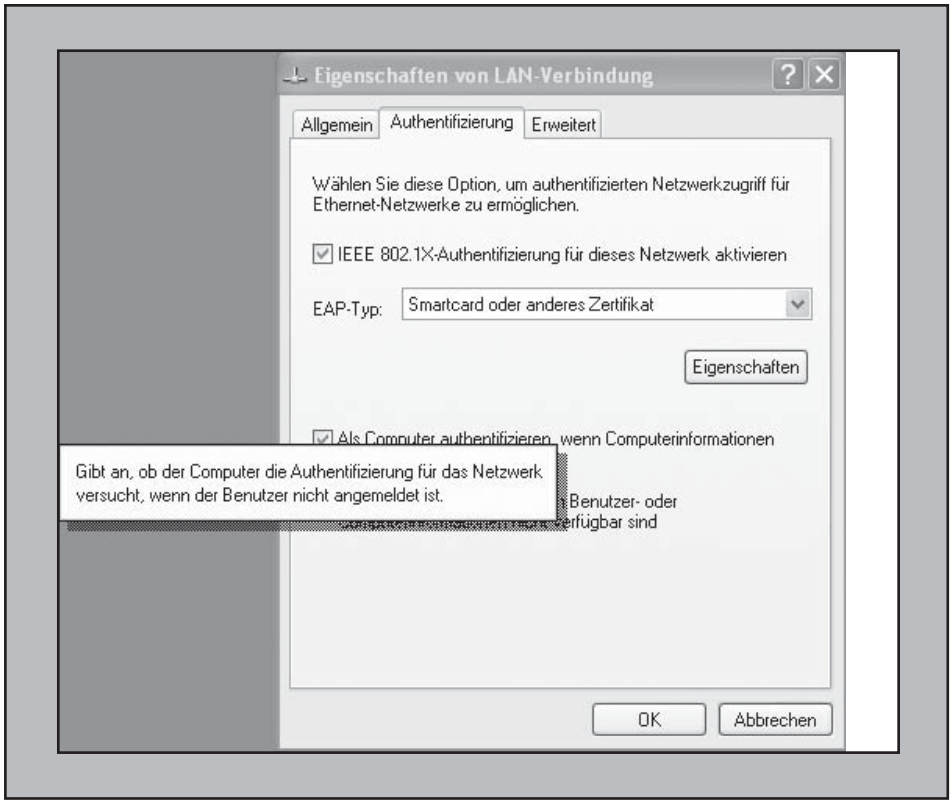


Abbildung 4.1: Aktivierung der Geräteauthentifizierung unter Windows XP

- zumindest wenn man das Passwort nicht im Klartext auf dem Client hinterlegen möchte. Doch selbst wenn man sich dafür entscheiden würde, müssen für diese Verfahren gerätespezifische „Benutzer"-Konten mit eigenen Passwörtern angelegt und gepflegt werden.

Ausnahmen und daher besser zur Geräteauthentifizierung geeignet sind:

- EAP-TLS, hierbei werden Clientzertifikate überprüft;
- EAP-FAST, hierbei wird ein Pre-Shared Key genutzt;
- EAP-SIM und EAP-AKA, hierbei werden Daten von SIM-Karten genutzt - dies setzt jedoch voraus, dass die SIM-Karten ohne PIN aktiviert werden können.

Zur Geräteauthentifizierung ist es also (selbstverständlich) erforderlich, dass der Authentication Server das Gerät über die gewählte EAP-Methode überhaupt authentifizieren kann! Das heißt, er muss je nach EAP-Methode auch über eine geeignete Datenbasis der Systeme verfügen.

Entscheidend, ob man sich für die Benutzer- oder Geräteauthentifizierung entscheidet, ist aber zunächst die Frage, wann das einzelne System Netzwerkzugriff benötigt: Bevor oder erst nachdem sich ein Benutzer angemeldet hat. Beispiele für einen Netzwerkzugriff ohne angemeldeten Benutzer sind:

- Wake-on-LAN,
- Softwareverteilungsroutinen,
- computerbasierte Richtlinien im Windowsnetz,
- lokale Ressourcen (wie z.B. Drucker), die im Netz freigegeben sind,
- zentrale Datensicherung lokaler Ressourcen,
- Serverdienste für das Netzwerk,
- öffentliche Angebote zur anonymen Nutzung wie beispielsweise ein Besucherinformationssystem an öffentlich zugänglichen PCs.

Darüber hinaus wird man schnell feststellen, dass es eine große Menge weiterer Geräte im Netzwerk gibt, die gar keine benutzerbasierte Authentifizierung sinnvoll zulassen. Hierzu gehören

- alle Server,
- Netzwerkdrucker,
- VoIP-Hardphones,
- Erfassungsgeräte wie Scanner, Zeiterfassungsterminals,
- Überwachungsgeräte wie Kameras,
- Steuerungstechnik,
- Produktionsmaschinen
- und viele mehr.

Zusammenfassend kann man über eine Geräteauthentifizierung sagen:

- Für eine flächendeckende Sicherheitslösung kann man in der Regel auf gerätebasierende Authentifizierungsverfahren nicht verzichten.
- Zu prüfen ist dann, wie die Vorteile einer ergänzende Benutzerauthentifizierung integriert werden können (siehe hierzu Kapitel 4.1.3).
- Wünschenswert sind Geräteauthentifizierungen über EAP-TLS.

1.1.2 Authentifizierung auf Basis der MAC-Adresse

Falls von bestimmten Clienttypen keine 802.1X-basierende Authentifizierung unterstützt wird, müssen hierfür am Zugangspunkt/Switch Ausnahmeregelungen geschaffen werden, die letztlich Löcher in den aufgebauten Schutzwall reißen.

Als Authentifizierungsverfahren auf niedrigster Stufe bieten für diesen Fall die meisten Produkten an, auf der Basis von MAC-Adressen zu authentifizieren. Auch hierbei unterstützen die meisten Switches und Access Point neben der Definition einer lokalen Accessliste auch die Möglichkeit, die MAC-Adressen über RADIUS von einem zentralen Authentifizierungsserver überprüfen zu lassen. Damit verliert man zumindest den Vorteil der zentralen Datenbasis nicht, das Verfahren kann nahtlos in eine RADIUS-Infrastruktur zur Authentifizierung eingebettet werden und eignet sich daher insbesondere als Einstiegs- oder Übergangsvariante bei der Einführung von 802.1X.

Insbesondere alle über RADIUS austauschbaren Informationen (siehe Kapitel 4.3) können vom Switch/Access Point und vom Authentifizierungsserver übermittelt und ausgewertet werden.

Offensichtlich ist jedoch das Authentifizierungskriterium „MAC-Adresse" kein geheimes Credential und kann daher leicht für Angriffe unter der Identität eines regulären Systems genutzt werden (MAC-Address-Spoofing). Dies ist das größte Problem an einer Authentifizierung via MAC-Adresse.

Zu beachten ist daher: Eine Authentifizierung über MAC-Adressen liefert zwar ein Accounting regulärer Benutzer bzw. Geräte und kann auch zur Trennung von Benutzergruppen verwendet werden, bietet aber für das entsprechende LAN-Segment keinen weiteren Schutz vor aktiven Angriffen!

Einige Produkte unterstützen pro Port eine Art Fall-Back der Authentifizierungsverfahren:

- Als Erstes wird über EAP-Request-Identity eine 802.1X-Authentifizierung gestartet,

- wird dieser Request innerhalb eines Timeout-Intervalls nicht beantwortet, wird (über RADIUS) versucht die MAC-Adresse zu überprüfen.

Eine solche sich automatisch zurückstufende Authentifizierung mag während einer Umstellungsphase hilfreich sein, ist aber sicherheitstechnisch zunächst nicht besser als eine MAC-Adressenbasierende Authentifizierung.

Hilfreich ist jedoch das folgende Szenario (siehe auch Abbildung 4.3): Alle über MAC-Adresse authentifizierten Geräte werden dynamisch einem separaten VLAN zugeordnet, welches höheren Sicherheitsbeschränkungen unterworfen ist und durch eine Firewall von restlichen LAN getrennt ist. Aber auch hierbei ist zu bedenken, dass damit alle Systeme in diesem VLAN untereinander nicht geschützt sind und dass es außerdem Angriffsszenarien gibt, die in der Lage sind VLAN-Grenzen zu überschreiten (VLAN-Hopping).

In jedem Fall sollte jedoch für LAN/WLAN-Segmente, in denen Wireless Clients eingesetzt werden müssen, die kein WPA oder 802.11i unterstützen und daher per MAC-Adresse authentifiziert werden, notwendigerweise ein eigenes isoliertes Netzsegment geschaffen werden, welches den gesamten Netzverkehr über eine geeignete Firewall leitet. Zu beachten ist hierbei außerdem, dass ohne WPA/802.11i auch keine sichere Verschlüsselung der übertragenen Daten gewährleistet ist!

Für Wireless LANs nach 802.11i fordert der Standard die Unterstützung dynamischer Schlüsselaustauschverfahren, wobei der PMK (siehe Kapitel 0) jedoch nicht notwendigerweise von einem EAP-Verfahren geliefert werden muss, sondern bei reduziertem Schutzbedarf auch als Pre-Shared Key fest vorgegeben werden kann. Dieses oft als WPA-PSK bezeichnete Verfahren liefert ein akzeptables Sicherheitsniveau, falls der Pre-Shared Key genügend komplex gewählt ist (mindestens 20 zufällige Zeichen), und kann durch die zusätzliche Überprüfung der MAC-Adressen ergänzt werden.

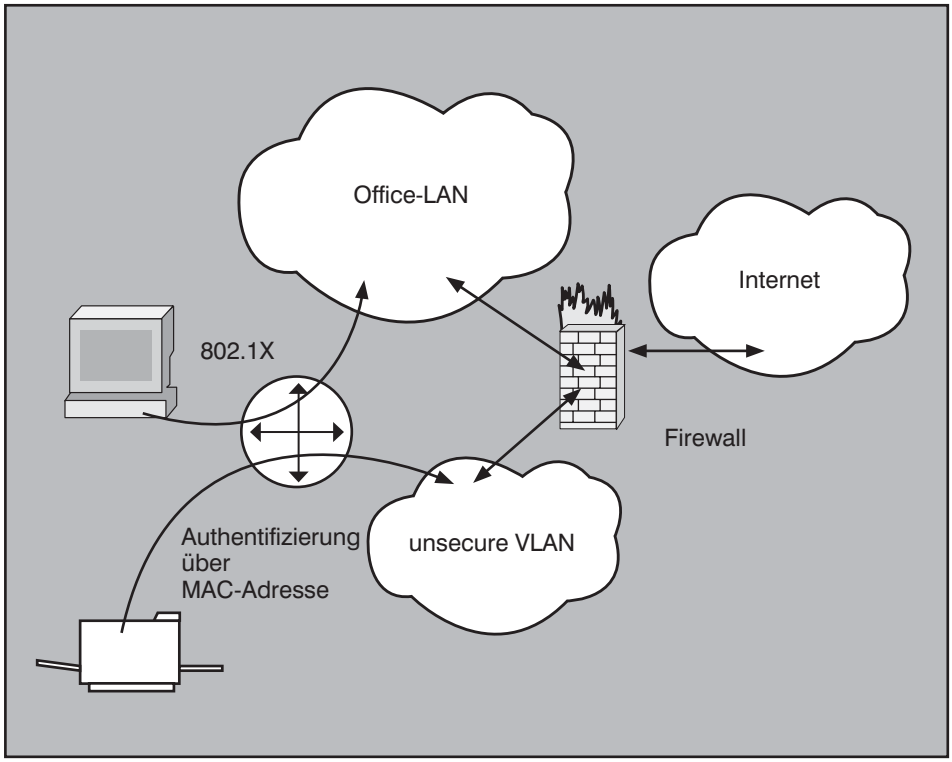


Abbildung 4.3: Trennung von sicher und unsicher authentifizierten Geräten

Schwerpunktthema

Hasta la VISTA Windows XP!

Mehrwert-potentiale von Windows Vista unabhängig betrachtet

Fortsetzung von Seite 1

Markus Holländer ist Competence Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH. Neben der Leitung des Competence Centers sind seine Hauptaktivitäten Projektleitungen, Konzipierungen und Reviews im Bereich der Themen Windows Server 2003 (Longhorn), Active Directory, DNS und Windows XP bzw. Vista für private und öffentliche Auftraggeber. Insbesondere zu diesen Themenkomplexen verfügt er über jahrelange Projekterfahrung bei namhaften Unternehmen und eine Vielzahl erfolgreich abgeschlossener Projekte. Die Projekte erstreckten sich von lokalen Kunden mit mehreren hundert bis hin zu globalen Implementierungen mit mehreren tausend Computern. Herr Holländer ist auch für die Entwicklung der Windows Server 2003 Seminare des Competence Centers in Zusammenarbeit mit der ComConsult Akademie verantwortlich und einer der Hauptreferenten.

Dipl.-Inform. Michael van Laak ist seit 1999 bei der ComConsult Beratung und Planung GmbH als Senior Berater im Competence Center Backoffice tätig. Zu seinen Spezialgebieten zählt das Design von Verzeichnisdiensten, die Migrationskonzipierung und -durchführung insbesondere Windows Umfeld (Active Directory, Windows Server 2003, XP, Vista), sowie die Erstellung und Implementierung von Administrationskonzepten. Herr van Laak verfügt über langjährige Erfahrung in der Durchführung und Leitung von nationalen und internationalen Projekten sowie als Referent von öffentlichen Seminaren und Inhouse Veranstaltungen.

Das Verhalten mit dem ersten Release Candidate (RC 1) war leider ähnlich. Auch wenn jedem eigentlich klar ist, dass eine neue Betriebssystemversion aus dem Hause Microsoft höhere Hardware-Anforderungen stellt, schien Vista ein regelrechter Performance-Killer zu sein. Und dann kam der RC 2. Auch hier wollen wir nicht übertreiben, aber subjektiv betrachtet „ging die Sonne auf“. Eigentlich schon mit der Installation (Standardinstallation in ca. 25 Minuten - Volumen ca. 7 GB) hat man den Eindruck, dass sich da einiges getan hat. Dies wird dann auch gleich bei ersten Kopiervorgängen bestätigt, seien es beispielsweise Kopiervorgänge von einer Festplatte auf einen Stick oder auch via Netzwerk, es geht gefühlt alles wesentlich schneller als mit XP. Dieses beschleunigte Verhalten wird auch sehr markant im Netzwerkumfeld auffallen. Dieser positive Eindruck bestätige sich auch mit der Nutzung der finalen Version von Vista. Diese Version wurde in den letzten Tagen der Artikelerstellung ebenfalls genutzt und konnte so noch im Rahmen dieses Artikels mit einbezogen werden. Ebenfalls folgt noch ein kurzer Blick in Richtung Office 2007, welches bei einem Rollout von Vista wohl oft in Kombination mit ausgerollt werden wird.

Vista im Netzwerk

Wie bereits in der Einleitung beschrieben, ist subjektiv sehr auffällig, dass sich einiges im Bereich des Netzwerks von Vista getan hat. Der Zugriff auf andere Rechner - speziell Server - und auch das Kopieren von Daten geht spürbar schneller. Microsoft hat mit Vista (und auch mit Longhorn auf der Serverseite) einen komplett neuen TCP/IP-Stack entwickelt. Dies trifft sowohl für IPv4 als IPv6 zu. Der so genannte „Next Generation TCP/IP-Stack“ weist insbesondere im Bereich der Performance verschiedenste Neuerungen auf. Eine dieser Neuerungen ist beispielsweise die „automatische Anpassung der TCP Receive Window Size“. Bei dieser Funktionalität wird permanent neu festgelegt, wie die optimale Window Size ist. Dies geschieht durch die ständige Überprüfung des Bandbreitenprodukts und der Abfragerate der Anwendung. Dies führt schließlich dazu, dass die Netzwerkbandbreite während der Datenübertragung besser genutzt wird. Insbesondere in Netzen mit hoher Bandbreite und großer Latenz bzw. mit einen großen Anzahl von verlorenen Paketen fällt die bessere Performance mit dem „Next Generation TCP/IP-Stack“ auf. Im Bereich Wireless LAN wird die Performance Verbesserung auch dadurch erreicht, dass da folgende RFCs unterstützt werden:

1. RFC 2582 die NewReno-Modifikation des TCP-Fast Recovery Algorithmus
2. RFC 2001 der Fast Recovery-Algorythmus
3. RFC 2883 die Erweiterung der SACK-Option von TCP
4. RFC 3517 ein SACK-basierter Loss Recovery-Algorythmus für TCP

Hasta la VISTA Windows XP! - Mehrwertpotentiale von Windows Vista unabhängig betrachtet

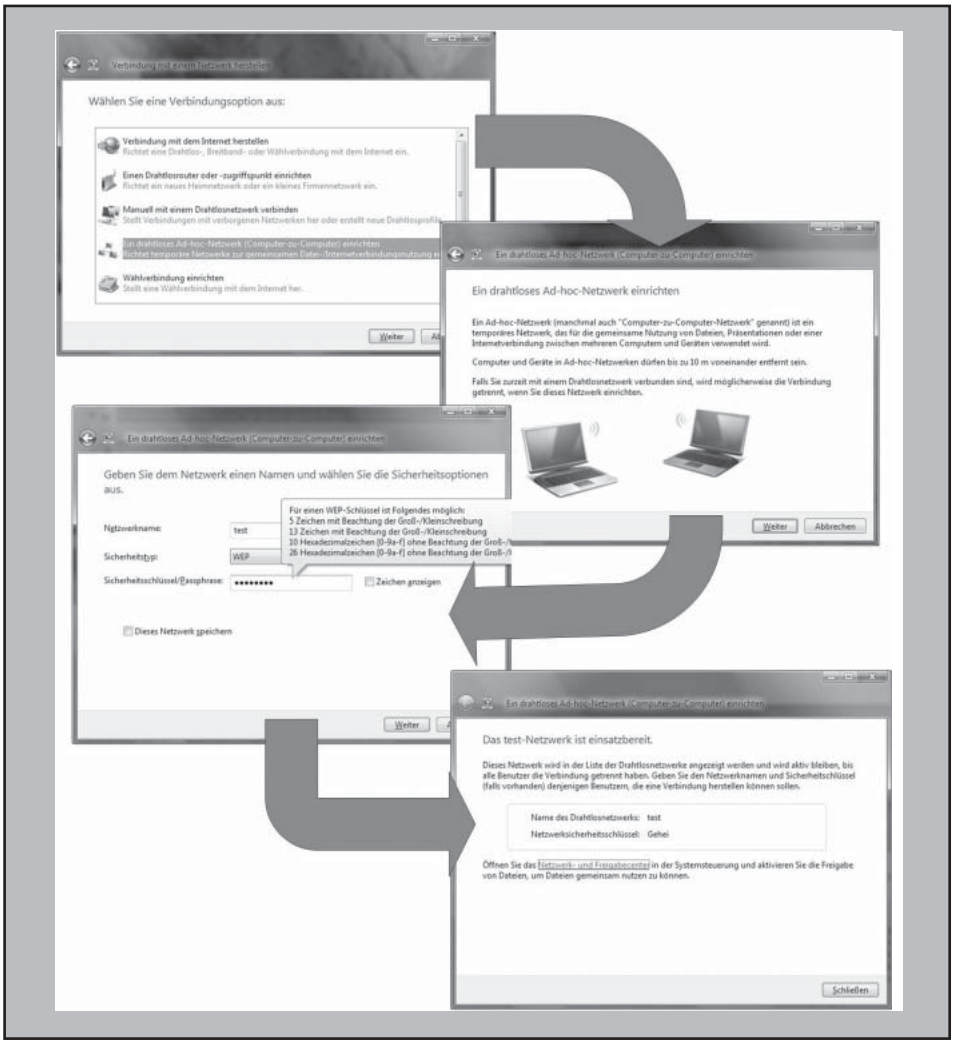


Abbildung 1: Adhoc-Netzwerk einrichten

Dabei ist der Anspruch der, dass es Personen mit wenig IT-Know-How ermöglicht wird, ein Adhoc Netzwerk aufzubauen. Ein Szenario, was dazu gerne einfällt, ist die Zusammenkunft mehrerer VIPs mit Notebooks, die mal eben ein Meeting abhalten möchten. In der Abbildung 1 „Adhoc-Netzwerk einrichten“ kann man die 4 Schritte sehen, die zur Einrichtung eines Adhoc-Netzes unter Vista erforderlich sind. Hierzu braucht man sicherlich nicht die Kenntnis, was beispielsweise eine IP-Adresse ist, allerdings ist es mit diesen Schritten noch nicht ganz getan, da noch die Freigabe von Daten erfolgen muss. Insofern erlöst dies die IT nicht von der Pflicht, auch weiterhin alle Benutzer zu schulen bzw. zu unterweisen. Es scheint jedoch einen Tick leichter zu werden.

Im Bereich der Netzwerkadministration hat Microsoft unter Vista ebenfalls eine neue Verwaltung integriert. Hier kann man geteilter Meinung sein, ob diese effektiver und einfacher zu bedienen ist. Jedenfalls ist das Erscheinungsbild ein ganz anderes. Im so genannten Netzwerk- und Freigabecenter erhält man eine Übersicht über alle aktiven Verbindungen und Informationen zu Freigaben. In Abbildung 2 sieht man eine Wireless-Verbindung (WASI) und eine VPN-Verbindung zu comconsult.com (CoCoVPN). Sollten, wie in der Abbildung durch das Kreuz dargestellt, vermeintliche Probleme vorliegen, dann kann man die Diagnose direkt von diesem Fenster aus starten (z.B. durch Klick auf das Kreuz). Durch die Verknüpfungen auf der linken Seite gelangt man zu den weiteren Administrationspunkten.

5. RFC 4138 Forward RTO-Recovery - ein Algorythmus zur Erkennung von falschen Retransmission-Timeouts für TCP und SCTP

Weitere Infos insbesondere auch zu den RFCs sind im Artikel „Verbesserungen im Next Generation TCP/IP-Stack im Bereich Leistung“ unter http://www.microsoft.com/germany/technet/datenbank/articles/600985.mspx zu finden.

Standardmäßig ist bei Vista IPv4 und IPv6 aktiviert. Dies wird durch eine Zweischichten-TCP/IP-Stack-Architektur unterstützt. Diese Unterstützung ermöglicht auch eine schleichende Migration unter Verwendung von IPv6-Übergangstechnologien, die den IPv6-Verkehr mittels eines Tunnels durch ein privates IPv4-Netzwerk leiten. Auch unterstützt Vista PPPv6 und virtuelle Netzwerke nach dem Layer 2 Tunneling-Protokoll (L2TP/IPv6). Laut Aussage von Microsoft wird auch IPv6 dazu genutzt, den Aufbau von Adhoc-Netzwerken zu vereinfachen.

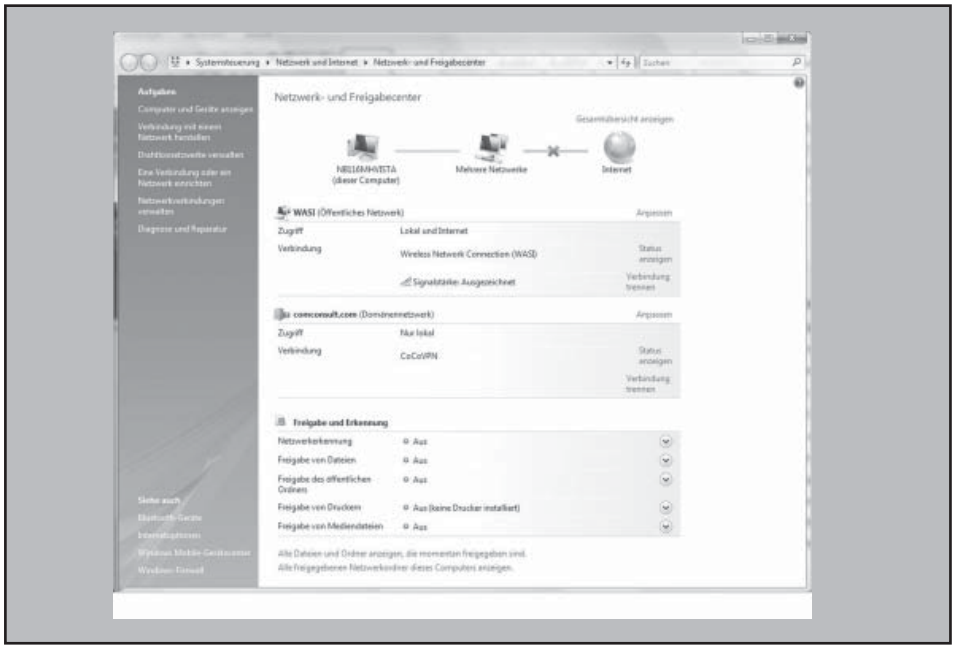


Abbildung 2: Netzwerk- und Freigabecenter

Hier kann man dann z.B. manuell ein sicherheitsaktiviertes drahtloses Netzwerk einrichten. Auffällig war hierbei allerdings, dass mittels des Assistenten nicht alle erforderlichen Konfigurationen gemacht werden konnten, sondern dass nach der Erstkonfiguration mittels weiterer manueller Anpassung noch ein Eintrag gesetzt wurde (der Sicherheitstyp musste noch eingestellt werden). Dies spricht ein wenig gegen die Vereinfachung. Insgesamt jedoch machen die teilweise neuen Verwaltungstools im Netzwerkbereich einen sehr guten Eindruck hinsichtlich der Handhabung und der Möglichkeiten. Insbesondere die neue Netzwerk Diagnose und Reparatur Möglichkeit wird den Anwendern helfen. Nach diesem kleinen Blick auf das Netzwerk, bei dem vordergründig nicht die offensichtlichsten Mehrwertpotentiale gesehen werden (es sei denn man hat ein spezielleres Szenario und möchte beispielsweise IPv6 nutzen) folgt nun ein Blick auf ein Feature von Vista, welches ein Mehrwert darstellen könnte: Die Laufwerksverschlüsselung mittels BitLocker.

Bitlocker

Mit diesem Ansatz zur Verschlüsselung setzt Microsoft auf die „Trusted Plattform Module“ (TPM), so dass entsprechende Hardware erforderlich ist. Hierbei ist aber besonders zu beachten, dass es TPM 1.2 sein muss, TPM in der Version 1.1 funktioniert nicht. Bei neuen Notebooks sollte jedoch eine TPM 1.2 Unterstützung vorhanden sein bzw. es sollte bei Neukauf darauf geachtet werden, dass ein solcher Chip integriert ist. Bitlocker ist nur in der Enterprise und Ultimate Version von Vista verfügbar. In den Testszenarien für diesen Artikel wurden ein DELL Latitude D 810 und ein D 620 verwendet. Da noch wenige Stunden vor Redaktionsschluss neueste Informationen zu Bitlocker in Erfahrung gebracht wurden, wurde auch noch nachträglich ein D 510 in das Testszenario einbezogen. Aus diesem Grunde sollte dieser Teil des Artikels auf alle Fälle bis zu Ende gelesen werden. Bei allen Laptops wurden die aktuellsten BIOS-Versionen und Vista Ultimate in der finalen Version verwendet. Wer das D 810 genau kennt, wird einwerfen, dass das Notebook nur einen TPM 1.1 besitzt. Das stimmt und war auch im Testumfeld nicht anders. Allerdings war die Konfiguration der Nutzung ohne TPM in der Vista Beta 2 möglich, was innerhalb der grafischen Benutzeroberfläche bzw. mittels des Verwaltungstools „Bitlocker Laufwerksverschlüsselung“ geschah. Ab RC 1 und auch in der finalen Version sollte eine Konfiguration mittels Befehlszeile möglich sein, aber dazu später mehr. Letztendlich dient aber der TPM Chip dazu, Schlüssel zu speichern.

Grundsätzlich wird mit Bitlocker das System sowohl offline, als auch während des Boot-Prozesses sowie bei der Nutzung geschützt. Zu bemerken ist, dass Bitlocker „nur“ für die Systempartition verwendet werden kann. Besitzt man 2 Partitionen (System und Data beispielsweise), dann muss die 2. Partition mittels EFS verschlüsselt werden, wenn man eingebaute Funktionalitäten verwenden möchte. Ein Offline-Schutz liegt vor, da alle Dateien (also auch die Dateien für den Ruhezustand und die Auslagerungsdatei) verschlüsselt sind. Während des Bootprozesses wird dann kontrolliert, ob die Bootdateien noch im korrekten Zustand sind. Externe Software, die beispielsweise über ein anderes Laufwerk gebootet wird, hat keinen Zugriff auf den TPM-Chip und somit nicht die Möglichkeit, an diese Informationen zu gelangen bzw. diese zu nutzen. Sollte die Festplatte aus dem Notebook ausgebaut werden, fehlen ebenfalls die Informationen vom TPM-Chip. Hier gilt aber anzumerken, dass es für Problemfälle auch Recovery-Optionen gibt.

Bei den Tests zu Bitlocker wurde zuerst die Option ohne einen geeigneten TPM-Chip gecheckt. Hierbei wird dann der Schlüssel auf eine USB-Stick gespeichert, der während des Bootvorgangs eingesteckt sein muss. Prinzipiell ist dies vom Ansatz her schon nicht die beste Lösung - insbesondere im Vergleich zur Lösung mit einem integrierten TPM-Chip, jedoch schien dies eine Alternative darzustellen. Im Vorfeld schien die „Windows Vista Beta 2 - Schritt für Schritt Anleitung zu Bitlocker Drive Encryption“ eine gute Grundlage zu sein (http://www.microsoft.com/germany/technet/prodtechnol/windowsvista/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.mspx). Aus diesem Grunde wurde zunächst genau nach dieser Anleitung vorgegangen. Zuerst wurde der „leere“ Rechner entsprechend den Anweisungen während des Vista-Installationsprozesses partitioniert. Erforderlich ist eine 1,5 GB große Partition (Volume für Startinformationen) und die eigentlich zu verschlüsselnde Partition (Betriebssystemvolume). Hierzu muss man ziemlich zum Anfang der Vistainstallation den Installation-Wizard zwischenzeitlich verlassen und mittels des Befehlszeilentools „diskpart“ die entsprechende Partitionen anlegen. Bei diesem Prozess wird auch das diskpart-Kommando shrink verwendet, was die Größe einer Partition verkleinern kann.

Hierzu noch zwei Nebensätze und einen passenden Testfall: Zum einen ist es in Vista jetzt möglich, die Partition zu verkleinern und zu vergrößern. Dies kann sogar online erfolgen und wird normalerweise innerhalb der Computerverwaltung in der Datenträgerverwaltung durchgeführt. Und zum anderen sollte man sich mit dem Tool „diskpart“ vertraut machen, da man dieses wahrscheinlich braucht, sobald man die Systemwiederherstellung benötigt - insbesondere bei Problemen mit Partitionen, Volumes, Disks etc. Der besondere Testfall, über den es sich zu berichten lohnt, ist die Nutzung der Partitionsverkleinerung. Grundsätzlich wurde die Funktion in allen Tests sehr gut bestätigt, manchmal

kann man jedoch nicht so viel verkleinern, wie nach einem Blick auf die noch ungenutzte Speicherkapazität vermutet. Führt man aber eine umfassendere Partitionsverkleinerung durch und startet den Rechner während dieses Vorgangs neu, dann ist er danach „erst einmal“ unbrauchbar. Vista weist auch nicht darauf hin, dass es damit Probleme geben könnte. Sämtliche Reparaturversuche innerhalb der Systemwiederherstellung z.B. die automatisch mit Vista integrierten Optionen oder auch diskpart schlugen in unserem Testumfeld fehl. Ebenfalls war das lesbare Einbinden der Platte unter Windows XP nicht möglich. Die Daten hätten schließlich damit gerettet werden können, indem man die Platte unter einer anderen laufenden Vistainstallation wieder einbindet (vorher ist ein manueller Import von Datenträgerinformationen erforderlich, der aber im Kontextmenü angeboten wird). Dies funktioniert natürlich nur so lange, wie die Daten nicht verschlüsselt sind (EFS oder Bitlocker). Alternativ hätte man natürlich auch eine Sicherung während der Systemwiederherstellung wieder einspielen können. An dieser Stelle noch der Hinweis, dass die Funktion „Complete-PC Sicherung“ in erster Linie in den Unternehmenversionen enthalten ist (Business, Enterprise, Ultimate). Diese Funktion konnte auch in sämtlichen Tests ohne negative Ergebnisse getestet werden. Man muss sogar erwähnen, dass die Sicherung und auch die Wiederherstellung auf eine oder von einer externen Festplatte sehr schnell funktionieren. Genaue dokumentierte Ergebnisse wurden nicht erfasst, jedoch wurden beim Restore mehr als 1 GB pro Minute wieder hergestellt (z.B. 48 Minuten für ca. 55 GB).

Aber nun zurück zur Bitlocker-Thematik und dem ersten Szenario. Nachdem Vista auf den speziell angelegten Partitionen fertig installiert wurde, wäre laut Anleitung der nächste Schritt gewesen, Bitlocker zu aktivieren. Wie aber bereits weiter oben geschrieben, wurde diese Funktion aus dem GUI ab dem RC 1 entfernt. Auch in der finalen Version ist diese Möglichkeit nicht mehr enthalten. Die weitere Recherche ergab, dass die Möglichkeit, ohne kompatiblen TPM Bitlocker zu nutzen, doch noch vorhanden zu sein scheint. Innerhalb des Windows Scripting Host existiert der Befehl „manage-bde“ (Beschreibung: Konfiguriert die Bitlocker-Laufwerkverschlüsselung auf Datenträgervolumes). Ein Teil der Hilfe zu „manage-bde“ wurde dem Kasten 1 hinzugefügt.

Darin kann auch der verwendete Befehl zur Aktivierung von Bitlocker für das beschriebene Szenario nachvollzogen werden. Der Befehl ist der ersten Zeile der Abbildung 3 zu entnehmen. Hiermit wurde die Laufwerksverschlüsselung für das Laufwerk C: eingeschaltet, der StartupKey wurde auf F:\ gespeichert (in diesem Beispiel war F:\ ein USB-Stick), und der Wiederherstellungsschlüssel mit Kennwort wurde in das Verzeichnis C:\bitlocker gesichert. Nach Ausführung dieses Befehls wurde der Rechner neu gestartet und im Anschluss begann die Verschlüsselung der Systempartition (C:\). Das Bitlockerverwaltungstool zeigte ebenfalls an, dass die Verschlüsselung gerade durchgeführt wurde, obwohl sie ja von dort aus nicht zu initiieren war. Ebenfalls konnte man einen genaueren Stand der Verschlüsselung mittels „manage-bde -status“ erfahren, wo ein prozentualer Anteil angezeigt wird. Laut GUI und Befehlszeile wurde die Verschlüsselung ordnungsgemäß durchgeführt. Man konnte auch problemlos arbeiten, ein erster Eindruck hinsichtlich der Performance ergab keine spürbare Änderung. Bootet man das System dann neu und lässt zum Check den USB-Stick raus, dann wurde ordnungsgemäß der Zugang verweigert und es wurde eine entsprechende Bitlocker-Meldung angezeigt. So weit, so gut! Steckte man den USB-Stick mit dem entsprechenden StartupKey jetzt ein, dann begann Vista zu starten, blieb aber nach einiger Zeit in einem undefinierten Zustand hängen (schwarzer Bildschirm). Ein Start im abgesicherten Modus ergab, dass Vista bei „crcdisk.sys“ hängt. Diese Aktion wurde mehrfach auf dem benannten System durchgeführt, jedesmal mit dem gleichen Ergebnis. Auch Reparaturversuche mittels Recoveryoptionen scheiterten. Das Notebook war somit unbrauchbar.

Es scheint also seine Gründe zu geben, warum Microsoft diese Option aus dem GUI entfernt hat. Unsere Empfehlung kann in diesem speziellen Fall nur lauten, dies mindestens nochmals zu testen, falls man Bitlocker in dieser Variante (kein TPM 1.2 vorhanden) einsetzen möchte, wobei die Tendenz aktuell nicht für eine Nutzung spricht. Der durchgeführte Blick auf „manage-bde“ war aber nicht umsonst, da man damit auch die TPM-unterstütze Variante administrieren kann (und dies auch skriptgesteuert und auf anderen Rechnern), was in Unternehmensumgebungen bei Verwendung von Bitlocker sicher erforderlich werden wird. Aber zu diesem Zeitpunkt war die gesamte Funktionalität noch ein wenig fraglich, so dass im zweiten Szenario der Test auf einem Notebook mit TPM 1.2 erfolgte. Die Partitionierung und die Installation von Vista erfolgten wie im ersten Szenario bereits beschrieben. Im Anschluss wurde zuerst die TPM-Nutzung im BIOS eingeschaltet. Hierbei ist darauf zu achten, dass das aktuellste BIOS verwendet wird, da es ggf. zu TPM noch Änderungen bzw. Korrekturen gibt. Ist die Nutzung von TPM jetzt im BIOS eingeschaltet, dann wird im Verwaltungsprogramm von Vista bzgl. TPM (tpm.msc) eine Initialisierung möglich, siehe hierzu Abbildung 4. Danach ist der Rechner neu zu starten und das BIOS fragt bzgl. der Modifikation an. Hat man dieser zugestimmt und der Rechner startet wieder neu, dann musste man im dargestellten Szenario anschließend nochmals in das BIOS gehen, um TPM auch zu aktivieren. Nach der Anmeldung muss man dann ein wenig aufpassen, denn der „TPM Initializa-

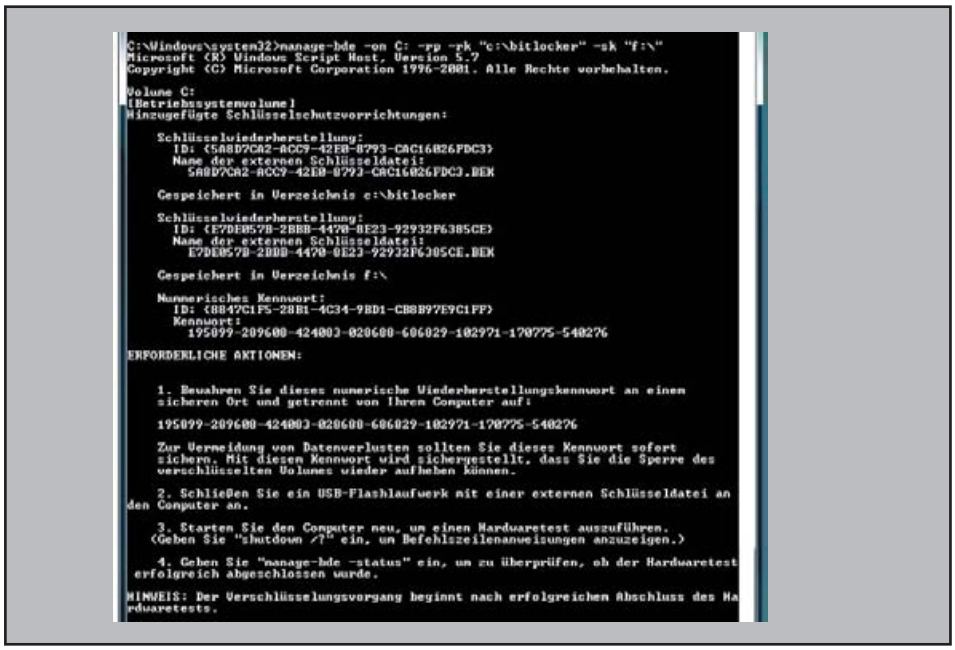


Abbildung 3: manage-bde zum Einschalten der Laufwerksverschlüsselung

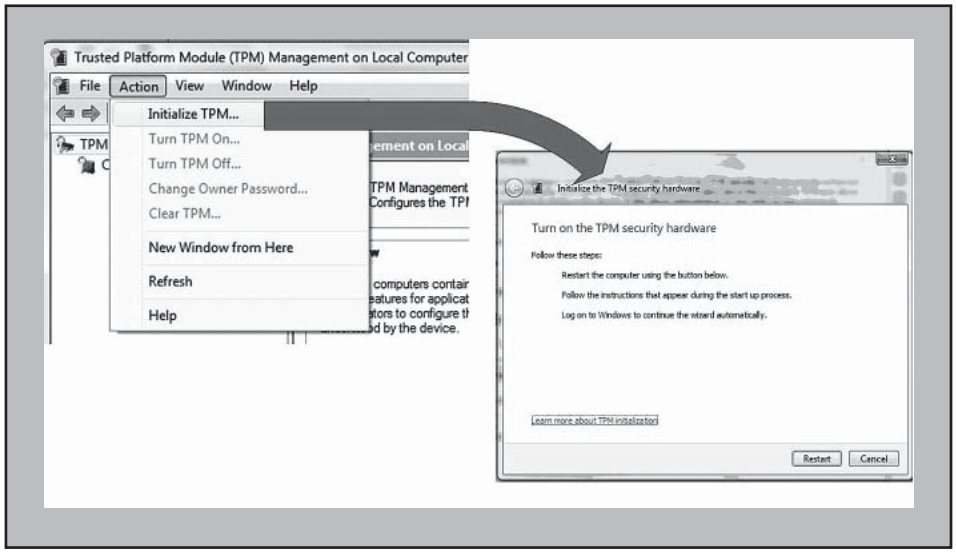


Abbildung 4: TPM initialisieren

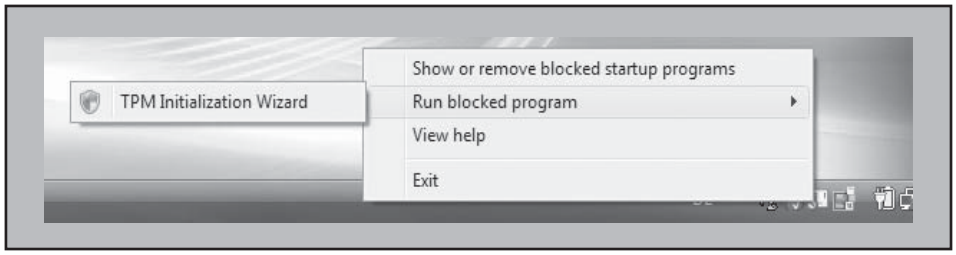


Abbildung 5: TPM Initialisierung wird zunächst geblockt

tion Wizard“ wird aus Sicherheitsgründen zunächst geblockt, siehe Abbildung 5.

Bei den weiteren Schritten definiert man dann die TPM-Ownership, sichert das Kennwort und bereitet den TPM-Chip zur Verwendung vor. Ist dies erfolgreich durchgeführt, kann man in der Verwaltung Bitlocker einschalten, siehe auch Abbildung 6. Ferner kann man dann das Recovery-Kennwort auf einen USB-Stick und in ein Verzeichnis sichern, sowie diese Informationen auch ausdrucken. Dies sollte natürlich auch tunlichst durchgeführt werden und die Informationen sollten auch tatsächlich an sicheren Orten gelagert werden. Zum Abschluss dieses Assistenten kann dann die Verschlüsselung gestartet werden. Laut Microsoft soll sogar ein Herunterfahren oder ein Neustart während der Durchführung der Verschlüsselung möglich sein, was auch erfolgreich getestet wurde. Möchte man neben der Nutzung von TPM auch noch zusätzlich einen PIN beim Start als zusätzlichen Authentifizierungsmechanismus nutzen, muss dies laut Hilfe bei der ersten Implementierung initialisiert werden. Dies wurde jedoch im Testumfeld nicht nachgestellt.

Abbildung 6: Bitlocker aktivieren

Im Gegensatz zum ersten Szenario funktionierte der Rechner auch nach dem ersten Neustart, und Vista startete erfolgreich. Da diese Tests erst kurz vor Redaktionsschluss beendet wurden, können hinsichtlich der Performance keine fundierten Aussagen getroffen werden, es scheint jedoch subjektiv so, dass die Verschlüsselung die Plattenzugriffe nicht spürbar verlangsamt. Insgesamt muss angemerkt werden, dass der gesamte Prozess vom ersten Einschalten von TPM im BIOS bis hin zur abschließenden Verschlüsselung mittels Bitlocker doch ziemlich kompliziert ist, so dass dies sicherlich kein „normaler“ Benutzer durchführen kann. Eine flächendeckende Implementierung ist genau zu betrachten, da man zur Initialisierung mehrfach ins BIOS muss und diverse Neustarts des Systems erforderlich sind. Ist allerdings Bitlocker einmal implementiert, kann es völlig transparent wirken und auch ein erhebliches Maß an Sicherheit bieten. Nicht zuletzt ist diese Funktionalität ohne Zusatzinstallationen bereits ins Betriebssystem integriert, zumindest in der Enterprise und Ultimate Version.

Ganz aktuell

Am Tag des Redaktionsschlusses wurde noch ein neuer „Step-by-Step Guide für BitLocker Drive Encryption“ bei Microsoft gesichtet (http://www.microsoft.com/downloads/details.aspx?FamilyID=311f4be8-9983-4ab0-9685-f1bfec1e7d62&DisplayLang=en#filelist). Im Gegensatz zum weiter oben bereits erwähnten Guide für die Beta 2 gibt es in diesem Guide doch einige Ergänzungen, die einen zusätzlichen Test rechtfertigten. Wie bereits für das 1. Szenario beschrieben, muss der Rechner entsprechend partitioniert werden. Im Gegensatz zur obigen Beschreibung wird jedoch nicht zuerst eine Partition angelegt, diese verkleinert und dann eine zweite Partition

angelegt, sondern es wird zuerst die kleine Partition für das „System Volume“ erzeugt, auf aktiv gesetzt und im zweiten Schritt (dahinter) die Betriebssystempartition erstellt.

Die eigentliche Entdeckung im Step-by-Step Guide war aber, dass es eine spezielle Gruppenrichtlinie zur Aktivierung der Bitlocker Verschlüsselung auf Rechnern ohne kompatiblen TPM gibt (siehe auch Abbildung 7). Im zweiten Test wurde diese Option entsprechend gewählt. Der Umstand, dass diese Gruppenrichtlinie nicht direkt gesehen wurde, zeigt einmal mehr, dass die Gruppenrichtlinien ein hervorragendes Werkzeug sind, um einen Computer den Feinschliff zu geben, aber auch, dass sie aufgrund der Anzahl und Komplexität nicht leicht zu managen sind. Aber zu den Gruppenrichtlinien später noch mehr.

Nach einem „gpupdate.exe /force“ zur Aktualisierung der Gruppenrichtlinien konnte auch tatsächlich auf einem Rechner ohne TPM Bitlocker im GUI aktiviert werden. Nach der Aktivierung wurden dann die Einstellungen für den Rechnerstart konfiguriert und auch die Recovery Optionen wurden festgelegt bzw. gesichert. Nachdem erforderlichen Neustart erfolgte dann die Verschlüsselung. Auch an dieser Stelle lief alles glatt. Nachdem die Verschlüsselung durchgeführt war, wurde der Rechner neu gestartet und man konnte ganz normal arbeiten, sofern man zum Systemstart die USB-Stick eingesteckt hatte. Um dem Benutzer ggf. die Arbeit zu erleichtern, sollte man das speziell für Bitlocker erstellte Laufwerk ausblenden.

Fazit Bitlocker

Natürlich kann nach dem beschriebenen Hin und Her zu Bitlocker kein abschließendes Statement erfolgen, auch sind die Gründe für das beschriebenen Fehlverhalten nicht klar. Allerdings wird grundsätzlich schon ein Mehrwert gegenüber Windows XP gesehen, wobei eine entsprechend durch Tests abgesicherte Planung als Voraussetzung angesehen wird - insbesondere wenn angestrebt wird, dies in die entsprechende Softwareverteilung bzw. das Deployment zu integrieren. Im nächsten Schritt wird Bitlocker auf verschiedenen Systemen (auch ohne kompatibles TPM) aktiviert, um dies weiter zu testen. Sollte ein Leser des Artikels Interesse an den weiteren Ergebnissen haben, so kann er dies gerne unter hollaender@comconsult.com anfragen.

Windows Vista Deployment

Die Mechanismen im Bereich Windows Deployment sind mit Windows Vista erstmalig grundlegend überarbeitet worden. Dies gilt insbesondere für die eigentliche Installation von Windows Vista, welche nun Image-basiert abläuft. Allerdings wurden ebenfalls im Umfeld der automatisierten Verteilung weitreichende Erweiterungen vorgenommen. Hier sind beispielsweise das „Windows Automated Installation Kit“ (WAIK) bzw. die „Business Desktop Deployment“ Suite (BDD) zu nennen. Eine Übersicht der einzelnen Deployment Komponenten sowie der generelle Ablauf bei der Installation eines duplizierten Master Clients wird im folgenden Abschnitt dargestellt. Die Einbindung in den Microsoft Systems Management Server wird im Rahmen dieses Artikels nicht betrachtet, zumal es ebenso möglich ist, die hier beschriebenen Mechanismen zur Image-basierten Installation von Windows Vista in die Softwareverteilungslösungen anderer Hersteller zu integrieren. Anschließend werden die einzelnen Schritte zur Durchführung eines Vista-Deployments näher betrachtet. Hierbei wird sowohl die manuelle Installation als auch die teilautomatisierte Verteilung über Netzwerk mittels „Windows Deployment Services“ (WDS) berücksichtigt.

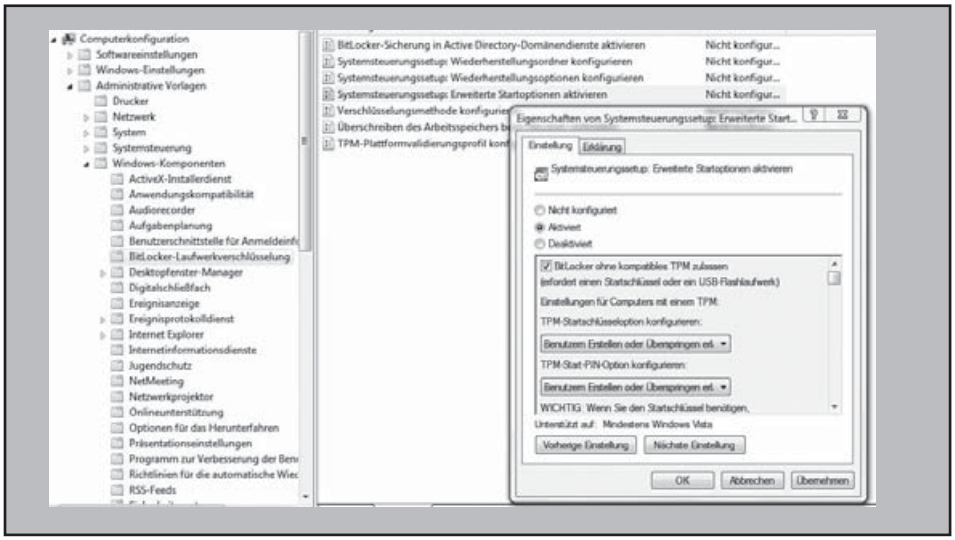


Abbildung 7: Bitlocker Gruppenrichtlinie „Erweiterte Startoptionen aktivieren“

Grundlagen

Die Windows Installation wird nun vollständig innerhalb einer grafischen Oberfläche (Windows PE) durchgeführt. Die Daten werden nicht mehr mittels klassischen Kopierens einzelner Dateien, sondern mittels eines Image-basierten Verfahrens auf die lokale Festplatte transferiert. Das hierfür verwendete Image auf der Windows Vista Installations-DVD enthält sämtliche Varianten von Windows Vista - es wird nur noch generell zwischen 32bit und 64bit unterschieden. Dieses Image ist nun komplett unabhängig vom verwendeten Zielsystem, insbesondere vom jeweiligen HAL-Typ. Dies ist ein signifikanter Vorteil gegenüber einer herkömmlichen Image-basierten Installation von beispielsweise Windows XP über Drittherstellertools, wo zumindest ein separates Image pro HAL-Typ benötigt wurde. Ebenso ist Windows Vista in der Enterprise- und Ultimate-Variante sprachunabhängig. Es muss also nicht mehr wie bei Windows XP die US-englische Version installiert sein, um (zusätzliche) internationale Sprachpakete nachinstallieren zu können. Es können nun modular beliebige Sprachpakete hinzugefügt oder entfernt werden. Somit entstehen auch für den internationalen Einsatz keine höheren Grundlizenzkosten mehr, wie dies bei der Multi-Language Version von Windows XP der Fall war. Achtung: Windows Vista Enterprise wird nur für Kunden erhältlich sein, deren PCs durch die Microsoft Software Assurance oder durch ein Microsoft Enterprise Agreement abgedeckt sind.

Je nach Unternehmen ist es also durchaus denkbar, den Standard-Client mit nur einem einzigen Image abdecken zu können, welches bereits Imaging-fähige Standard-Applikationen enthalten kann und folgende Zielkonstellationen abdeckt:

- Desktop PC (ACPI, UP, MP/UP)
- Notebook (ACPI, UP, MP/UP)
- Unterschiedliche Sprachpakete

Für einen geplanten Rollout von Windows Vista sollte man sich also frühzeitig mit den neuen Deployment Mechanismen beschäftigen, da sich ein optimaler Rolloutprozess für Windows Vista mit Sicherheit von den bisher gewohnten Rolloutprozessen für ältere Windows Versionen grundlegend unterscheiden wird.

Deployment Komponenten

Bevor nun detailliert auf den Ablauf eines beispielhaften Deployment Zyklus eingegangen wird, sollen zunächst kurz die benötigten Komponenten vorgestellt und der generelle Ablauf skizziert werden.

BDD

Der „Microsoft Solution Accelerator for Business Desktop Deployment" ist eine Suite von Tools und Dokumentationen für die Bereitstellung, Konfiguration und automatisierte Verteilung von Windows Vista und Standardsoftware. Die BDD Suite kann auf der Microsoft Connect Seite kostenlos heruntergeladen werden (http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx).

WAIK

Das „Windows Automated Installation Kit" ist Teil des BDD und enthält Tools für die Erstellung und Verwaltung von eigenen Vista Distributionen. Windows PE ist ebenfalls im WAIK enthalten und steht somit nun für jeden frei zur Verfügung.

ImageX

Dieses Tool (ursprünglich XImage in früheren Beta Versionen von Vista) ist Bestandteil des WAIK und ermöglicht die Verwaltung von WIM Files (Windows Imaging). Innerhalb der WIM Files werden die Daten über einen Single Instance Store (SIS) verwaltet. Dies ist der Grund dafür, dass auch bei Bereitstellung sämtlicher Vista Varianten auf der Installations-DVD die Datei „install.wim" nur unwesentlich größer ist als eine WIM Datei mit nur einer einzigen Vista Variante. Mittels ImageX können bestehende WIM Files in ein Verzeichnis gemountet und auch bearbeitet werden. Somit können bestehende Images gepflegt werden, ohne das Image auf einen Client ausrollen zu müssen, dort die gewünschten Änderungen vorzunehmen und dann ein neues Image generieren zu müssen. Es lassen sich so nicht nur Dateien in das WIM File hinein kopieren, sondern auch Betriebssystem Patches oder Service Packs slipstreamen. Das Imaging Verfahren arbeitet dateibasiert, wodurch eine nicht-destruktive Anwendung auf eine bestehende Partition möglich ist. Es kann also der Inhalt einer Image Datei den bestehenden Daten auf einem Datenträger hinzugefügt werden, ohne den aktuellen Inhalt zu löschen (ggf. natürlich überschreiben!).

WinPE

Das „Windows Preinstallation Environment" ist im WAIK enthalten und somit jetzt für jeden kostenlos zugänglich. Mittels WinPE können bootfähige Datenträger (CD, DVD, USB Wechselmedien) mit einer auf Windows basierenden grafischen Oberfläche erzeugt werden. Dies wird in der Regel zu Installationszwecken oder für Desaster Recovery Szenarien genutzt.

WDS

Die „Windows Deployment Services" sind fester Teil des Windows Longhorn Servers bzw. als Teil des WAIK auch auf Windows Server 2003 installierbar. WDS ist die Weiterentwicklung von RIS („Remote Installation Services") und stellt eine PXE-basierte Bootumgebung mit über Netzwerk bootbaren Images zur Verfügung. Auf dieser Basis können weitere Deployment Tasks durchgeführt werden, beispielsweise das Erzeugen eines Master-Client Images auf dem Deployment Share oder aber auch das Verteilen dieses Images auf neue Rechner.

PXE

Dies ist die Abkürzung für „Preboot Execution Environment". PXE wird verwendet, um vor dem Laden des Betriebssystems ausführbare Programme von einem Server zu empfangen und auszuführen. Dabei kann es sich um Wartungstools, Betriebssysteminstallationen oder ein eigenes Menü des PXE Servers handeln, in dem dann weitere Möglichkeiten zur Verfügung stehen.

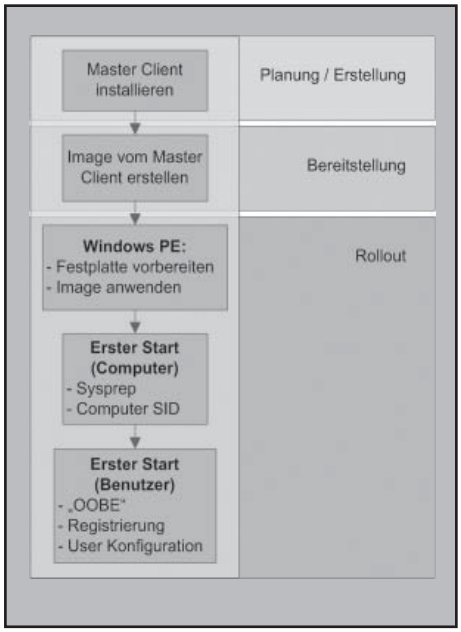


Abbildung 8: Ablauf eines manuellen Deployment Workflows

Windows System Image Manager

Dieses Tool mit grafischer Oberfläche zur Erstellung und Verwaltung von Images im „Windows Imaging" Format (WIM) ist Bestandteil des WAIK.

Sysprep

Tool zum Vorbereiten eines Master Clients für die Verteilung. Sysprep ist unter Windows Vista fester Bestandteil des Betriebssystems (unter Windows XP Teil der Support Tools).

Deployment Workflow

Generell lässt sich der einfachste Ablauf eines Deployment Zyklus wie in Abbildung 8 darstellen. Hierbei bezieht sich die Bezeichnung „einfach" auf die Komplexität des Workflows - nicht auf die notwendigen manuellen Schritte bei dieser Form des Rollouts.

Erstellung und Verteilung eines Master Clients

Im Folgenden werden die einzelnen Phasen des beschriebenen Deployment Workflows näher betrachtet. Hierbei soll zwischen einer manuellen Variante und einem teilautomatisierten Ansatz mithilfe von WDS unterschieden werden. Microsoft fasst beide Varianten unter dem Begriff „Lite Touch" Installation zusammen. Eine vollautomatisierte Installation bietet Microsoft nur in Kombination mit dem SMS 2003 OSD Feature Pack an und nennt dies dann „Zero Touch" Installation. Im Rahmen dieses Artikels wird zunächst eine manuelle Erstellung und Verteilung des Master Images beschrieben, um die Arbeitsweise der verwendeten Werkzeuge zu verdeutlichen. Auch bei späterem Einsatz von automatisierten Verteilungsmethoden erfolgt das Erstellen und Verteilen des Master Images im Hintergrund über die gleichen Mechanismen.

Master Client erstellen

Zunächst wird - wie auch bei der Erstellung eines Master Clients für frühere Windows Versionen - ein Referenzrechner bzw. Master Client aufgesetzt und nach Wunsch vorkonfiguriert. Hierbei muss nun jedoch nicht mehr zwischen Desktop und Notebook bzw. generell zwischen verschiedenen prozessorabhängigen HAL Typen (Hardware Abstraction Layer) unterschieden werden. Falls außer dem Betriebssystem weiterhin auch eine Sammlung von Standardapplikationen im Master Client enthalten sein, so bleibt natürlich

auch weiterhin zu testen, ob diese Applikationen Imaging-fähig sind. Unproblematisch sind hierbei in der Regel Anwendungen wie Microsoft Office oder Standard Tools wie Acrobat Reader. Einige Applikationen wie beispielsweise bestimme VPN Clients oder Virenscanner ließen sich jedoch in der Vergangenheit nicht fehlerfrei mittels Cloning verteilen.

Master Image erstellen

Nachdem der Master Client fertig installiert und konfiguriert ist, muss er mittels Sysprep auf die Duplizierung vorbereitet werden. Dieses Tool war bisher Teil der Support Tools und ist mit Vista direkt in die Betriebssysteminstallation integriert (zu finden auf der Systempartition im Ordner \Windows\system32\sysprep). Nach dem Start von Sysprep muss die Check Box „Verallgemeinern“ aktiviert werden, um die Generierung einer neuen Computer SID auf dem Zielsystem zu erzwingen. Weiterhin sollte die Option „Herunterfahren“ (nicht: „Neustart“) ausgewählt werden, um ein versehentliches Neustarten des Master Clients zu verhindern (siehe Abbildung 9).

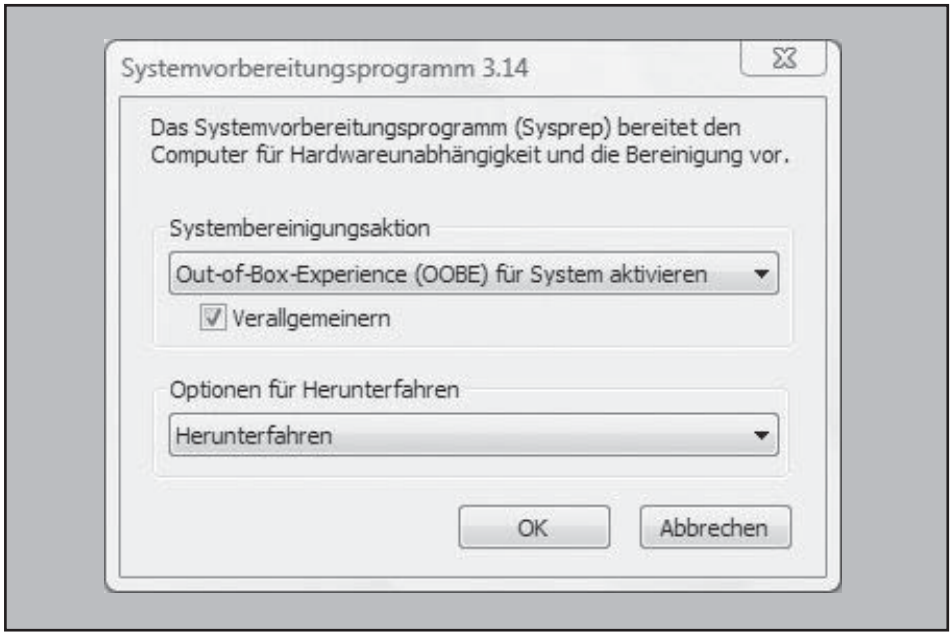


Abbildung 9: Sysprep Optionen

Im nächsten Schritt wird mittels ImageX die Systempartition in ein WIM File geschrieben. Hierfür kann man beispielsweise von der Windows Vista Installations-DVD booten und die System Recovery Tools starten (siehe Abbildung 10). Dort findet man unter Anderem auch die Option, eine Eingabeaufforderung zu starten. Hier kann nun beispielsweise ein USB Wechseldatenträger angeschlossen werden, auf dem sich ImageX befindet und auf den auch das WIM File abgelegt werden kann.

Abbildung 10: Microsoft Vista Recovery Tools starten

Das WIM-File wird mithilfe des folgenden Kommandozeilenbefehls erzeugt, wobei hier C: das zu clonende Systemlaufwerk und F: der angeschlossene USB Wechseldatenträger als Ziel des WIM Files namens „image.wim“ ist:

imagex /capture c: f:\image.wim “Master Client”

Hierbei wird das angelegte Image innerhalb des WIM Files mit “Master Client” benannt. Das Image kann dabei optional unter Verwendung des Parameters /compress auch noch komprimiert werden. Das so erzeugte WIM File kann nun für die Verteilung des Master Clients auf beliebige Zielsysteme verwendet werden.

Falls ein WDS Server zur Verfügung steht, kann der komplette Vorgang der Erstellung des Master Images auch per PXE Boot über das Netzwerk durchgeführt werden.

Optional: Master Image pflegen

Mit ImageX ist es möglich, WIM-Files in ein Verzeichnis zu mounten. Anschließend können beispielsweise zusätzliche Treiberdateien für neue Hardware per Filecopy hinzugefügt werden. Darüber hinaus kann das Tool pkgmgr genutzt werden, um Patches oder Service Packs in das Windows Verzeichnis zu slipstreamen.

Somit kann das Master Image aktualisiert werden, ohne es zunächst auf einen Client installieren zu müssen, dort die Updates durchzuführen und anschließend per Sysprep und ImageX neu zu verpacken.

Manuelle Verteilung des Master Images

Zunächst muss auf dem Zielcomputer eine entsprechend große aktive Partition existieren. Dies kann beispielsweise unter Windows PE erfolgen, indem man wie oben bereits beschrieben von der Vista Installations-DVD bootet. Alternativ ist es auch möglich, mithilfe der im WAIK enthaltenen WinPE Tools einen eigenen bootfähigen Wechseldatenträger (USB Stick,

USB Disk, CD, DVD) zu erstellen, welcher dann ebenfalls genutzt werden kann. In der WinPE Eingabeaufforderung verwendet man dann das Tool diskpart, um die Festplatte über die folgenden Befehle vorzubereiten, falls „disk 0“ die gewünschte Zielfestplatte ist und dort eine Partition namens „System“ über die komplette Festplattengröße erstellt werden soll:

```
select disk 0
create partition primary
select partition 1
format fs=ntfs label=“System“ quick
exit
```

Anschließend kann das vorbereitete Image auf die Zielpartition gespielt werden. Falls wie im obigen Beispiel ein externer Wechseldatenträger mit dem Laufwerksbuchstaben F: die Imagedatei enthält, muss hierfür der folgende Befehl verwendet werden:

```
imagex /apply f:\image.wim 1 c:\
```

Hierbei bitte nicht die “1” hinter dem Imagenamen vergessen - sie gibt an, welches Image innerhalb des WIM-Files verwendet werden soll. Zur Erinnerung: Es können mehrere Images in einem WIM-File abgelegt werden.

Nach Beendigung des Transfers muss der Computer neu gestartet werden. Auf einem DELL Inspiron 510 dauerte dieser Transfer ca. 10 Minuten. Im nun folgenden Mini-Setup werden noch einige wenige Informationen wie Computername, Zeitzone etc. abgefragt sowie ein Performance Test des Computers zur Bestimmung des Leistungsindex durchgeführt. Alles in allem war der oben genannte Rechner nach ca. 30 Minuten einsatzbereit.

Verteilung des Master Images mittels WDS

Wenn mehr als eine Handvoll Computer ausgerollt werden sollen, ist ein höherer Automatisierungsgrad und natürlich die Loslösung von lokal anzuschließenden Wechseldatenträgern erwünscht. Dies kann mithilfe der Windows Deployment Services (WDS) erreicht werden. WDS wird fester Bestandteil des Windows „Longhorn“ Servers sein, kann aber auch als Add-On für Windows Server 2003 bei Microsoft heruntergeladen werden (Bestandteil des WAIK, s.o.).

WDS stellt eine PXE Bootumgebung mit konfigurierbarem Boot Menü zur Verfügung. Es können beliebige Boot-Images und beliebige Installations-Images importiert werden (jeweils WIM Files). Als Boot Image kann beispielsweise die Datei boot.wim von der Windows Vista Installations-DVD verwendet werden. Ebenso kann aber auch mittels WAIK Tools ein eigenes WinPE Boot-Image erstellt werden. Entsprechend kann die Datei install.wim von der Vista DVD oder alternativ ein selbst erstelltes Image für die Installation verwendet werden (siehe auch Abbildung 11). Die Erstellung des Installations-Images kann auch direkt über das Netzwerk auf den WDS Server erfolgen. Eine detaillierte Schritt-für-Schritt Anleitung ist in der WAIK Dokumentation enthalten.

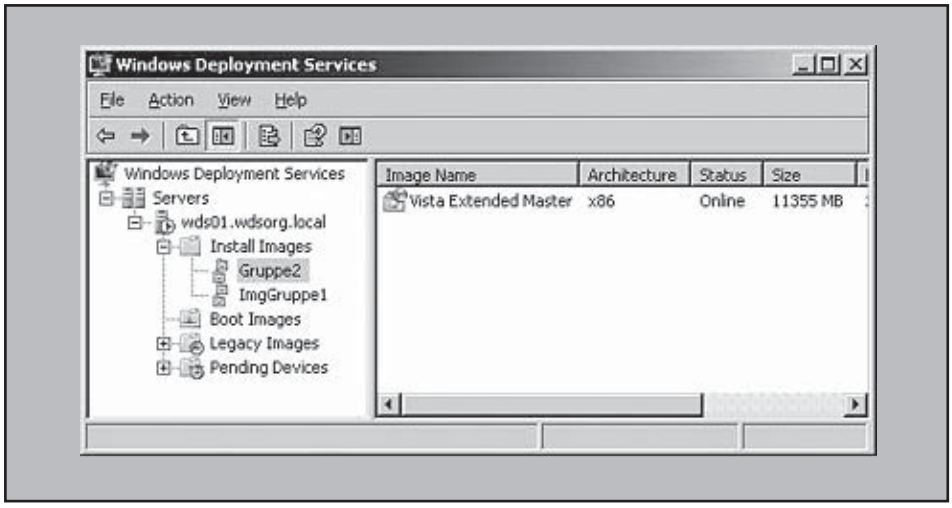


Abbildung 11: WDS Verwaltungskonsole

Anschließend sind im PXE Boot Menü die bereitgestellten Boot Images auswählbar. Falls nur ein einziges Boot Image bereitgestellt wird, startet dies automatisch. Im weiteren Verlauf kann das gewünschte Installations-Image verwendet werden. Interessant hierbei ist, dass nur die für den jeweiligen Computer passenden Images angezeigt werden (also beispielsweise nur die 32bit Varianten). Zur Erinnerung: Die WIM Images sind zwar unabhängig vom HAL Typ des Zielcomputers, allerdings muss zwischen der 32bit und der 64bit Variante von Windows Vista unterschieden werden.

Nachdem das Image kopiert ist, erfolgt die Personalisierung der Installation äquivalent zur manuellen Verteilung bzw. Standardinstallation von Windows Vista, falls keine Informationen für ein unattended Setup bereitgestellt

wurden. Dies kann über die Erstellung einer entsprechenden XML Antwortdatei erfolgen, welche mithilfe des WAIK generiert und verwaltet werden kann.

Fazit Deployment

Mit der Einführung eines File-basierten, nicht destruktiven und HAL Typ unabhängigen Imaging Verfahrens für das Windows Deployment hat Microsoft die erste gründliche Innovation seit der Bereitstellung von eigenen Deployment Mechanismen getätigt. Dass dies tatsächlich funktioniert, beweist die Auslieferung von Windows Vista eben auf Basis eines Master Images (\sources\install.wim).

Das „Drumherum“ wie BDD & Co. ist nichts grundlegend Neues, allerdings deutlich überarbeitet und leichter bedienbar als bisher. Für kleine Umgebungen ist es nun durchaus denkbar, den Client Rollout hinreichend komfortabel mithilfe der hier angesprochenen Komponenten durchzuführen. Es ist jedoch zu beachten, dass „Rollout“ nicht gleich „Client Management“ ist. Sämtliche Wartungsaufgaben wie zusätzliche Softwareinstallationen oder Patch Management sind damit noch nicht abgedeckt. Auch hierfür stellt Microsoft eigene Lösungen bereit, die teilweise kostenlos sind („Softwareverteilung“ mittels GPOs, WSUS). Hier muss allerdings sorgfältig geprüft werden, ob letztendlich eine solche Gesamtlösung hinsichtlich Leistungsfähigkeit und Administrierbarkeit die gestellten individuellen Anforderungen erfüllen kann. Wie gesagt, in kleinen Umgebungen sind solche Konstrukte durchaus denkbar.

In größeren Umgebungen wird man allerdings auch weiterhin oft nicht auf eine umfassende Softwareverteilungslösung verzichten können, welche sämtliche angesprochenen Bereiche abdeckt und zusätzlich weitere Features wie beispielsweise Lizenzmanagement etc. bietet. Dies muss aber sicherlich nicht unbedingt der Microsoft SMS sein - auch wenn Microsoft dies natürlich favorisiert. Auch weiterhin sind Kombi-Lösungen aus Imaging und Paket-basierter Softwareverteilung denkbar, wobei der Image-basierte Anteil nun durchaus mittels WIM Files abgedeckt werden kann, wodurch je nach aktuell verwendetem Imaging Verfahren die Flexibilität deutlich steigen kann.

Gruppenrichtlinien

Gruppenrichtlinien (Group Policy Objects - GPO) werden bereits in den beiden letzten Windows Generationen für die zentrale Konfiguration von Computer- und Benutzereinstellungen genutzt. Auch mit Windows Vista wird dieses Instrument weiterhin genutzt - allerdings wiederum stark erweitert und mit neuem Design versehen. So gibt es nun an die 3000 Richtlinien, unter anderem jetzt zur vollständigen Konfiguration der Windows Firewall und Einschränkungen bei der Geräteinstallation - um nur zwei Beispiele zu nennen. Eine detaillierte Beschreibung der Architektur und Arbeitsweise von GPOs unter Windows Vista kann unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/policy/policy/group_policy_start_page.asp eingesehen werden.

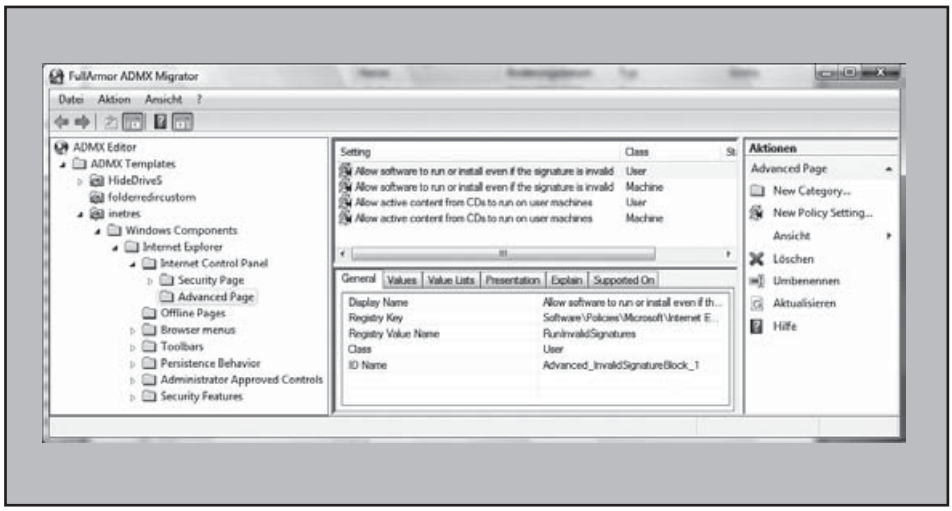


Abbildung 12: Der ADMX Migrator ermöglicht die Erstellung neuer .admx Vorlagen und die Migration bestehender .adm Vorlagen

Neues Format

Die grundsätzliche Architektur einer Gruppenrichtlinie ist für Windows 2000 und Windows XP Administratoren durchaus wiederzuerkennen. Allerdings werden die administrativen Vorlagendateien nun im XML Format verwaltet. Gleichzeitig wurden die Dateiendungen von .adm in .admx geändert. Microsoft hat ein Tool zum Migrieren von bestehenden .adm Vorlagendateien in das neue Format sowie zur Erstellung neuer .admx Vorlagen von der Firma Full Armor lizenziert. Dieses Tool heißt ADMX Migrator (siehe Abbildung 12) und ist als kostenloser Download erhältlich unter: http://www.microsoft.com/downloads/details.aspx?FamilyID=0f1eec3d-10c4-4b5f-9625-97c2f731090c&DisplayLang=en.

Neue Features

Ein interessantes neues Feature, für das bisher Drittherstellertools genutzt werden mussten, ist die Möglichkeit, die Verwendung von USB Devices differenziert zu handhaben. So kann es beispielsweise unerwünscht sein, dass USB Wechseldatenträger angeschlossen und verwendet werden können. Eine generelle Abschaltung der USB Schnittstelle jedoch würde auch keine Geräte wie Maus, Tastatur etc. zulassen, was natürlich nicht in Frage kommt. Nun ist es möglich, einzelne Geräteklassen gezielt zu verbieten (oder natürlich auch: alle bis auf einzelne). Um bei dem Beispiel Wechseldatenträger zu bleiben, wäre dies die Geräteklasse „DiskDrive“. Die Geräteklasse-GUID hierfür ist {4d36e967-e325-11ce-bfc1-08002be10318}. Dies kann im Geräte Manager auf der Karteikarte „Details“ in den Eigenschaften des Wechseldatenträgers nachgesehen werden. (siehe Abbildung 13)

Die Konfiguration erfolgt im Gruppenrichtlinieneditor unter „Computer / Admi-

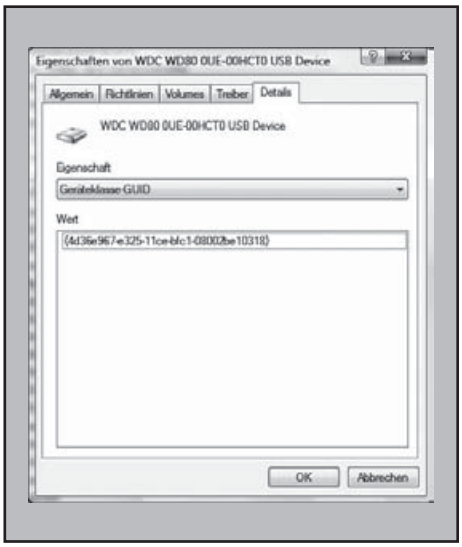


Abbildung 13: Die Geräteklasse-GUID kann im Geräte Manager nachgesehen werden

nistrative Vorlagen / System / Geräteinstallation / Einschränkungen bei der Geräteinstallation“, wo beispielsweise bestimmte Geräteklassen verboten werden können. Zusätzlich kann festgelegt werden, ob Administratoren von dieser Einschränkung ausgenommen werden sollen. In Abbildung 14 ist eine Konfiguration dokumentiert, in der es auch für Administratoren nicht möglich ist, Wechseldatenträger zu installieren.

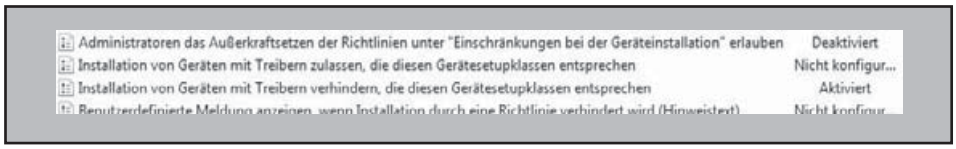


Abbildung 14: Konfiguration von Einschränkungen bei der Geräteinstallation (hier auch für Administratoren)

Die Konfiguration der verbotenen Geräteklassen erfolgt in den Eigenschaften der Richtlinie „Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen“ (siehe Abbildung 15). Hier muss die Geräteklasse-GUID eingetragen werden. Hinweis: Zum sofortigen Aktivieren dieser Computerrichtlinie anschließend in der Eingabeaufforderung „gpupdate /force“ eingeben.

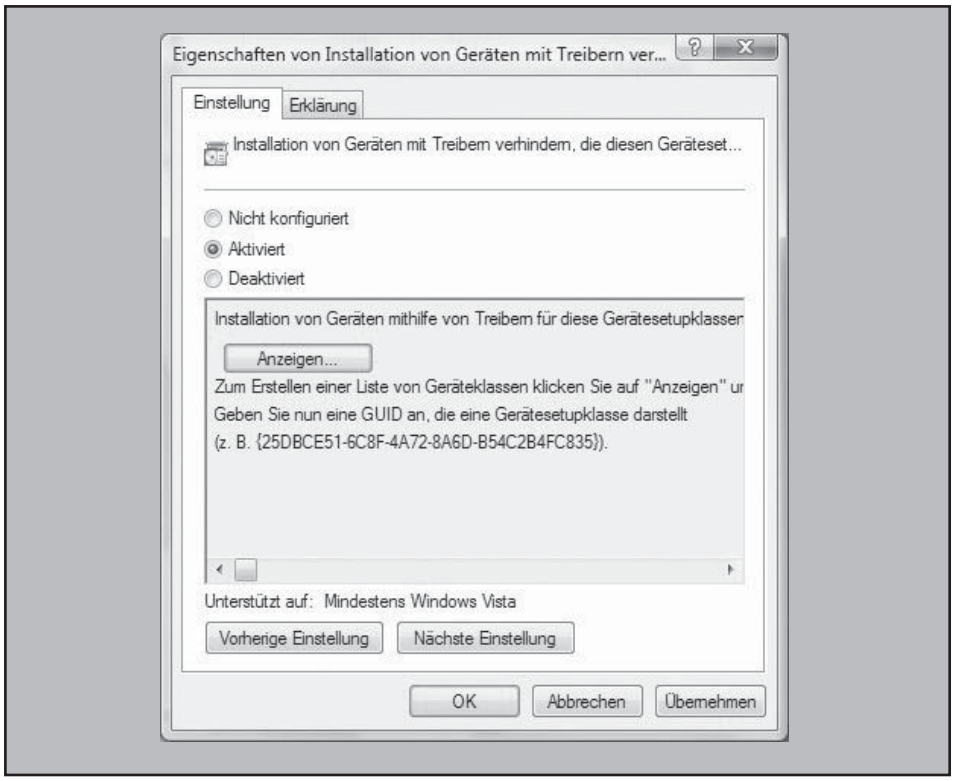


Abbildung 15: Durch Betätigen des Buttons „Anzeigen“ kann die Liste der verbotenen Geräteklassen-GUIDs seditiert werden.

Wenn anschließend ein USB Wechseldatenträger angeschlossen wird (z.B. ein USB Stick, siehe Abbildung 16), so kann dieser nicht verwendet werden, wobei der Hinweis auf eine entsprechende Richtlinienkonfiguration ausgegeben wird.

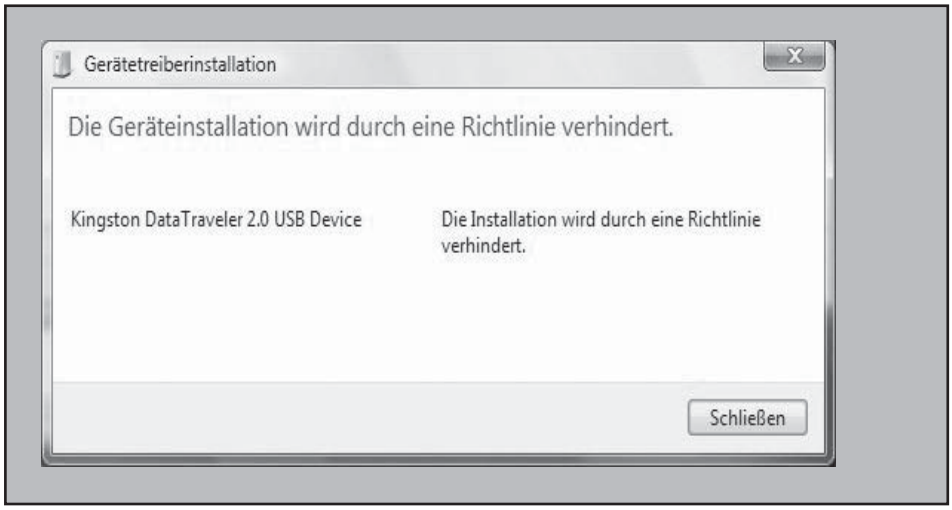


Abbildung 16: Die Verwendung eines USB Sticks wird nun verweigert

Fazit Gruppenrichtlinien

Die Umstellung auf ein XML-basiertes Dateiformat für administrative Vorlagen bleibt für den Administrator weitgehend transparent, da der ADMX Migrator für die Migration bestehender selbst erstellter Vorlagen sowie für die Neuerstellung eigener Vorlagen genutzt werden kann. Dies ist in kurzer Zeit und weitgehend intuitiv möglich.

Das Pro und Contra hinsichtlich der zahlreichen neuen Richtlinien in Windows Vista bleibt gleich in Bezug auf entsprechende Erweiterungen von Windows 2000 zu Windows XP: Man kann nun vieles einstellen, was man schon lange einstellen wollte, man muss es nur finden.

Office 2007

Noch ein paar Worte - allerdings auch wirklich nicht mehr - zu Office 2007. Gibt es mit Vista schon gravierende Änderungen im Look and Feel, werden diese mit Office noch verstärkt. Insbesondere in den Standard-Office-Anwendungen wie Word, Excel, Outlook und Powerpoint ändern sich die Symbolleisten und die gesamte Menüstruktur (siehe auch Abbildung 17).

Laut eigener Aussage hat Microsoft dies gemacht, um das ganze übersichtlicher zu gestalten. Natürlich gibt es auch neue Funktionen oder bekannte Optionen, die angepasst wurden, so dass dies erforderlich schien. Fakt ist, dass sich der Anwender neu orientieren muss. Allerdings muss man sagen, dass sich die Personen hier im Testbetrieb sehr schnell an das neue Office gewöhnt haben. Natürlich sucht man am Anfang oft nach dem einen oder anderen Feature, da es nicht mehr an der vermuteten Stelle liegt, doch dies gibt sich sehr schnell.

Hasta la VISTA Windows XP! - Mehrwertpotentiale von Windows Vista unabhängig betrachtet

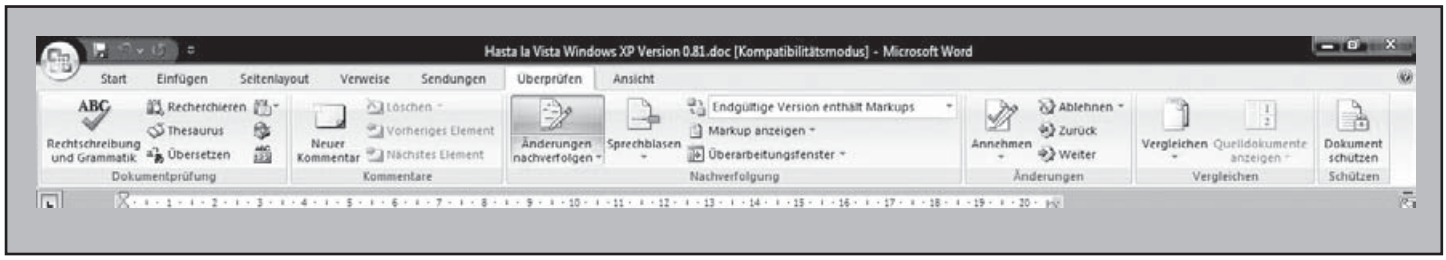


Abbildung 17: Neue Symbolleiste unter Word

Allerdings wird mit Office 2007 bzw. 2007 Microsoft Office System viel mehr angestrebt. Die bekannten „Flagschiffe“ wie Excel werden mehr und mehr Frontend für andere Applikationen und auch die Thematik Präsenzinformationen rückt mehr in den Mittelpunkt. Auch wird das Thema der Portale strategisch mehr und mehr forciert. Nicht zuletzt wird auch der Einstieg in die Telefonie inkl. Unified Messaging mit Office (Office Communicator und Outlook) vorangetrieben. Dies sind die Themen, die sowohl Office als auch dann letztendlich Vista nach vorne bringen. Dies zu beleuchten ist sicher Thema eines gesonderten Artikels.

Und noch vieles mehr

Im Artikel wurden bereits einige Neuerungen von Vista angesprochen, doch gibt es eine Reihe von erwähnenswerten Features bzw. Funktionalitäten, die nicht genannt wurden. Keine Angst - diese werden jetzt nicht aufgelistet, aber es gibt doch noch ein paar Hinweise. Zudem sind im Kasten 2 noch ein paar ausgewählte Features und die unterstützte Hardwareausstattung hinsichtlich RAM und unterstützter Anzahl von Prozessoren der Vista-Versionen gegenüber gestellt. Man sollte sich auf alle Fälle die Thematik Sicherheit genau anschauen: hier sind eine ganze Reihe neuer Funktionen hinzukommen, angefangen von der „User Account Control“, über Windows Defender, der Firewall bis hin zum beschriebenen Bitlocker. In diesem Zusammenhang steht natürlich auch der neue Internet Explorer 7, über den sogar die CT titelte „Der Nachzügler holt auf“. Nicht zuletzt lohnt sich auch ein Blick auf „Windows Live OneCare“. Damit wird Microsoft wohl auch in den Markt für Antivirenprodukte einsteigen.

Was das neue Design betrifft, kann man wie immer geteilter Meinung sein, aber hinsichtlich der Informationsfindung ist die Sidebar eine nette Ergänzung. Für den Benutzer am effektivsten ist aber die „Suche starten“ Funktionen direkt über im Startmenü. Hier werden alle Programme, Verzeichnisse und Dateien durchsucht und dies geht rasend schnell. Es wird wohl nicht lange dauern, bis man fast nur noch dort den Programm- oder Tool-Namen eintippt, um diese zu starten.

Auch im Netzwerkbereich gibt es noch verschiedenste Punkte, die man sich anschauen sollte. Ebenso die Treiberinstallation (insbesondere in diesem Zusammenhang „Windows Update“) ist zu betrachten, da hier auch positive Erfahrungen aus dem Testlabor vorliegen. Ob sich ein Blick auf die weiteren teilweise netten Spielereien lohnt, ergibt sich aus den persönlichen Vorlieben. Gerne hätten wir im Testumfeld noch die „SideShow“-Funktionalität getestet. Hierbei handelt es sich um ein zusätzliches kleines Display bei Laptops (ähnlich einem Telefon mit 2 Displays), auf denen weitere Informationen z.B. hinsichtlich Mails, Terminen, Batteriestand, aber auch ggf. zukünftig Telefonfunktionalität integriert werden kann. Leider war jedoch keine entsprechende Hardware auf dem Markt verfügbar.

Fazit

Kann man wirklich „Hasta la VISTA Windows XP!“ sagen? Man könnte es so formulieren: XP kann schon mal langsam anfangen zu packen. Mit Sicherheit wird jetzt nicht sofort die ganze Welt auf Vista schwenken, auch wenn Microsoft mit allen Mitteln versucht, eine Aufbruchsstimmung zu erzeugen. Doch es wird wohl wieder traditionell ablaufen, wobei dann die neuen Funktionen von Vista (z.B. im Bereich Deployment) ihr übriges tun werden. Der Druck wird über die Office-Schiene entstehen, insbesondere dann, wenn es Microsoft gelingt, auf der Messaging-Seite noch mehr Marktanteile zu generieren und auch der Einstieg in die Telefonie nur ansatzweise gelingt. So wird sich das Ganze dann gegenseitig hochschaukeln - und dann heißt es nicht nur „Hasta la Vista Windows XP!“, sondern es wird wahrscheinlich noch eine ganze Reihe anderer Produkte verschwinden.

Parameterliste zu manage-bde (Hilfe):

-status	Stellt Informationen zu BitLocker-fähigen Volumes bereit.
-on	Verschlüsselt das Volume und aktiviert den BitLocker-Schutz.
-off	Entschlüsselt das Volume und deaktiviert den BitLocker-Schutz.
-pause	Hält die Verschlüsselung oder Entschlüsselung an.
-resume	Setzt die Verschlüsselung oder Entschlüsselung fort.
-lock	Verhindert den Zugriff auf durch BitLocker verschlüsselte Daten.
-unlock	Lässt den Zugriff auf durch BitLocker verschlüsselte Daten zu.
-autounlock	Verwaltet die automatische Aufhebung der Sperre von Datenvolumes.
-protectors	Verwaltet die Schutzmethoden für den Verschlüsselungsschlüssel.
-tpm	Konfiguriert die TPM (Trusted Platform Module) des Computers.
-ForceRecovery or –fr	Erzwingt, dass ein mit BitLocker geschütztes Betriebssystem beim Neustart wiederhergestellt wird.
-ComputerName or –cn	Wird auf einem anderen Computer ausgeführt. Beispiele: „ComputerX“, „127.0.0.1“
-? or /?	Zeigt eine kurze Hilfe an. Beispiel: „-Parametersatz -?“
-Help or -h	Zeigt eine vollständige Hilfe an. Beispiel: „-Parametersatz -h“, siehe hierzu auch das folgende Beispiel zu manage-bde -on -help

manage-bde -on Volume

[{-RecoveryPassword|-rp} [NumericalPassword]]
[{-RecoveryKey|-rk} PathToExternalKeyDirectory]
[{-StartupKey|-sk} PathToExternalKeyDirectory]
[{-TPMAndPIN|-tp} PIN]
[{-TPMAndStartupKey|-tsk} PathToExternalKeyDirectory]
[{-EncryptionMethod|-em}
{aes128_diffuser| aes256_diffuser| aes128|aes256}]
[{-ComputerName|-cn} ComputerName]
[{-?|/?}] [{-Help|-h}]

Beschreibung manage-bde -on:

Verschlüsselt das Volume und aktiviert den BitLocker-Schutz. Verwenden Sie Parameter, um Schlüsselschutzvorrichtungen für den Verschlüsselungsschlüssel hinzuzufügen. Mit diesen Schutzvorrichtungen kann die Sperrung des Zugriffs auf durch BitLocker verschlüsselte Daten aufgehoben werden. Eine TPM-Schutzvorrichtung wird dem Betriebssystemvolume automatisch hinzugefügt, wenn der Computer über ein unterstütztes TPM verfügt. Für das Betriebssystemvolume beginnt die Verschlüsselung beim nächsten Neustart nach einem Hardwaretest.

Parameterliste:

Volume Erforderlich. Laufwerkbuchstabe gefolgt von einem Doppelpunkt (z. B. „C:“)

- RecoveryPassword or –rp

Fügt eine Schutzvorrichtung in Form eines numerischen Kennworts hinzu. Wenn der Parameter noch nicht hinzugefügt wurde, ist er zum Start der Verschlüsselung erforderlich. Lassen Sie das Argument leer, um ein zufälliges numerisches Kennwort zu generieren (empfohlen). Für diese Kennwörter gelten spezielle Formatanforderungen. Geben Sie Argumente mit der Option „?“ an, um die entsprechenden Anforderungen anzuzeigen.

- RecoveryKey or -rk

Fügt eine Schutzvorrichtung in Form eines externen Schlüssels zur Wiederherstellung hinzu (optional). Geben Sie den absoluten Verzeichnispfad an, unter dem die Datei mit dem zufällig generierten externen Schlüssel gespeichert werden soll. Beispiel: „E:“

- StartupKey or -sk

Fügt eine Schutzvorrichtung in Form eines externen Schlüssels für den Start hinzu. Der Parameter ist erforderlich, wenn auf dem Computer kein unterstütztes TPM vorhanden ist und noch nicht hinzugefügt wurde. Wenn ein Systemstartschlüssel verwendet werden soll, muss sich die gespeicherte Datei im Stammverzeichnis eines USB-Flashlaufwerks befinden. Da externe Schlüssel mit den Parametern „-RecoveryKey“ und „-StartupKey“ gleichermaßen generiert werden können, sind die gespeicherten Dateien austauschbar und können in beiden Fällen verwendet werden.

- TPMAndPIN or -tp

Fügt eine aus TPM und PIN bestehende Schutzvorrichtung für das Betriebssystemvolume hinzu (optional). Geben Sie als Argument die 4- bis 20-stellige numerische PIN an, die bei jedem Computerstart eingegeben werden muss. Da diese Schutzvorrichtung durch einen ausschließlichen TPM-Schutz außer Kraft gesetzt wird, werden alle TPM-Schutzvorrichtungen entfernt und ersetzt.

- TPMAndStartupKey or -tsk

Fügt eine TPM- und Systemstartschlüssel-Schutzvorrichtung für das Betriebssystemvolume hinzu (optional). Wenn ein Systemstartschlüssel verwendet werden soll, muss sich die gespeicherte Datei im Stammverzeichnis eines USB-Flashlaufwerks befinden.

Da diese Schutzvorrichtung durch einen ausschließlichen TPM-Schutz außer Kraft gesetzt wird, werden alle TPM-Schutzvorrichtungen entfernt und ersetzt.

• EncryptionMethod or -em
Konfiguriert den Verschlüsselungsalgorithmus und die Schlüsselgröße, die für ein unverschlüsseltes Volume verwendet werden. Wählen Sie eine der folgenden Einstellungen aus: AES 128 Bit mit Diffuser („aes128_diffuser“), AES 256 Bit mit Diffuser („aes256_diffuser“), AES 128 Bit („aes128“) oder AES 256 Bit („aes256“). Sofern keine andere Einstellung ausgewählt wurde, werden Datenträger mit „AES 128 Bit mit Diffuser“ verschlüsselt.

• SkipHardwareTest or -s
Beginnt die Verschlüsselung ohne einen Hardwaretest (optional). Wenn dieser Parameter nicht angegeben ist, müssen Sie den Computer neu starten und einen Hardwaretest erfolgreich abschließen, bevor auf dem Betriebssystemvolume mit der Verschlüsselung begonnen wird. Beim Test wird überprüft, ob das TPM wie erwartet funktioniert und ob der Computer beim Startvorgang eine externe Schlüsseldatei von einem USB-Gerät lesen kann.

• ComputerName or -cn
Wird auf einem anderen Computer ausgeführt. Beispiele: „ComputerX“, „127.0.0.1“

Kasten 1: Bitlocker und manage-bde

Unterschiedliche Features der Vista Editionen (Auszug)					
	Home Basic	Home Premium	Business	Enterprise	Ultimate
Hardware					
Anzahl (separater) CPUs	1	1	2	2	2
RAM (32bit)	4 GB	4 GB	4 GB	4 GB	4 GB
RAM (64bit)	8 GB	16 GB	> 128 GB	> 128 GB	> 128 GB
Oberfläche					
Zusätzliche Sprachpakete	-	-	-	+	+
Design Windows Vista Basic	+	+	+	+	+
Design Windows Aero	-	+	+	+	+
Datensicherung					
Backup-Scheduler	-	+	+	+	+
Komplette Systemsicherung	-	-	+	+	+
Shadow Copy	-	-	+	+	+
Versionswiederherstellung (Ordner / Dateien)	+	+	+	+	+
Sicherheit					
User Account Control	+	+	+	+	+
Jugendschutzeinstellungen	+	+	-	-	+
BitLocker (Festplattenverschlüsselung)	-	-	-	+	+
EFS (Dateiverschlüsselung)	-	-	+	+	+
Firewall / Defender	+	+	+	+	+
Netzwerk					
Domänenmitgliedschaft möglich	-	-	+	+	+
IPv6 Unterstützung	+	+	+	+	+
Next-Generation TCP/IP Stack	+	+	+	+	+
Gleichzeitige SMB Verbindungen	5	10	10	10	10
Remote Desktop	nur Client	nur Client	+	+	+
Sonstiges					
Erweiterter Laptop-Support	-	+	+	+	+
Windows Media Center	-	+	-	-	+

Kasten 2: Features zu Vista und Hardwareanforderungen

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Windows Vista - Tatsächlich Mehrwerte vorhanden?, 07.02.07 in Köln

Microsoft hat Ende November 2006 die finale Version von Windows Vista freigegeben und stellt diese auch für Unternehmenskunden zur Verfügung. Ende Januar 2007 kommt Vista dann in den Handel. Was haben Unternehmen von dieser neuen Version des führenden Betriebssystems zu halten? Schafft es Microsoft, mit der Etablierung von Vista die Basis für seine „people ready software“ zu legen? Welche Mehrwertpotentiale bietet Vista, insbesondere wenn man schon Windows XP im Unternehmen eingeführt hat?

Preis: € 990,- zzgl. MwSt.

IP-Telefonie evaluieren, planen, betreiben, 12.02. - 14.02.07 in Köln

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet. Preis: € 1.690,- zzgl. MwSt.

Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 12.02. - 16.02.07 in Aachen

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren. Preis: € 2.290,- zzgl. MwSt.

Quality of Service - QoS, 12.02. - 13.02.07 in Köln

Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standards es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert. Preis: € 1.390,- zzgl. MwSt.

EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren, 13.02. - 14.02.07 in Bonn

Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehende Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird. Preis: € 1.390,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 26.02. - 27.02.07 in Bonn

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

Konvergente Netze, 26.02. - 27.02.07 in Bonn

Im diesem 3-tägigen Seminar werden sowohl die Einflüsse der Konvergenzfelder und Technologien auf das Design der Unternehmensnetze diskutiert, als auch die Potentiale, die sich daraus ergeben. Preis: € 1.690,- zzgl. MwSt.

Ethernet-Netzwerke, 26.02. - 02.03.07 in Aachen

Dieses Seminar stellt die neuesten Ethernet- und Wireless-Varianten vor und zeigt, nach welchen Regeln und Auslegungsvorschriften diese zu konfigurieren sind. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, auch wichtige Betriebsfragen werden vorgestellt. Im Besonderen wird die Bedeutung der IP-Telefonie für die Gestaltung von Ethernet-LANs analysiert. Abgerundet wird das Seminar um wichtige Fragen des Trouble-Shootings. Preis: € 2.290,- zzgl. MwSt.

TCP/IP und SNMP, 26.02. - 02.03.07 in Berlin

Dieses 5-tägige Seminar vermittelt systematisch die Grundlagen TCP/IP, beleuchtet Vor- und Nachteile und gibt wichtige Empfehlungen für den erfolgreichen Einsatz. Dies betrifft speziell auch die wichtigen IP-Infrastrukturdienste von der Adressierung über ARP bis zu DHCP, DNS, DDNS und NAT und die Management-Funktionalität SNMP. Preis: € 2.290,- zzgl. MwSt.

Cisco Router erfolgreich einsetzen für Einsteiger, 26.02. - 02.03.07 in Aachen

Dieses 5-tägige Intensiv-Seminar vermittelt den optimalen Einsatz von Cisco-Routern in Kombination mit der erfolgreichen Handhabung der wichtigsten Routing-Verfahren. Typische Fehler und Tücken in der Konfiguration werden erklärt und Empfehlungen für eine erfolgreiche Konfiguration gegeben. Preis: € 2.350,- zzgl. MwSt.

WAN-Planung für zentrale Dienste, 26.02. - 28.02.07 in Berlin

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess, dem auch dieses 3-tägige Seminar dienen soll. Preis: € 1.690,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 01.03. - 02.03.07 in Köln

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
05.02. - 09.02.07 in Aachen
16.04. - 20.04.07 in Aachen
25.06. - 29.06.07 in Aachen
15.10. - 19.10.07 in Aachen
03.12. - 07.12.07 in Aachen

TCP/IP und SNMP
26.02. - 02.03.07 in Berlin
21.05. - 25.05.07 in Aachen
15.10. - 19.10.07 in Berlin

Internetworking
05.03. - 09.03.07 in Aachen
07.05. - 11.05.07 in Aachen
17.09. - 21.09.07 in Aachen
10.12. - 14.12.07 in Aachen

Ethernet Technologien - neuester Stand
26.02. - 02.03.07 in Aachen
21.05. - 25.05.07 in Aachen
10.09. - 14.09.07 in Aachen
26.11. - 30.11.07 in Aachen

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

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
12.03. - 16.03.07 in Aachen
11.06. - 15.06.07 in Aachen
03.09. - 07.09.07 in Aachen
12.11. - 16.11.07 in Aachen

Trouble Shooting in konvergenten Netzwerken
23.04. - 27.04.07 in Aachen
18.06. - 22.06.07 in Aachen
17.09. - 21.09.07 in Aachen
19.11. - 23.11.07 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
29.01. - 02.02.07 in Aachen
07.05. - 11.05.07 in Aachen
22.10. - 26.10.07 in Aachen

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

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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung
12.02. - 16.02.07 in Aachen
18.06. - 22.06.07 in Bonn
10.09. - 14.09.07 in Berlin

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
05.03. - 07.03.07 in Bonn
25.06. - 27.06.07 in Berlin
15.10. - 17.10.07 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
16.04. - 20.04.07 in Aachen
27.08. - 31.08.07 in Aachen
03.12. - 07.12.07 in Aachen

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

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

Impressum

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

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

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