ComConsult Research

Der Netzwerk Insider

Februar 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

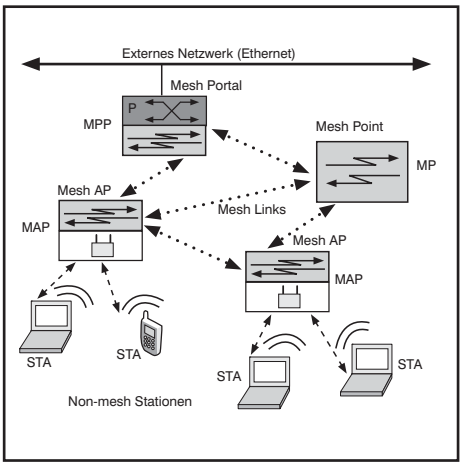
Vermaschte Wireless Netze:
Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s - Teil 1

von Dipl.-Inform. Petra Borowka

1. Motivation und Übersicht

Seit etwa Mitte 2005 entsteht ein Markt für die Weiterentwicklung von WLAN Produkten hin zu einer verteilten funkbasierten Architektur mit funktechnisch vermaschten Access Points unter dem Namen „Vermaschtes WLAN“ (Mesh WLAN). Diese „Mesh Architektur“ benötigt nur noch wenige, bei Bedarf redundante Übergangspunkte vom drahtlosen zum drahtgebundenen Netz. (siehe Abbildung 1.1)

Eigentlich nahm die Entwicklung vermaschter WLAN‘s ihren Anfang schon Mitte der 90er Jahre als Forschungsprojekt der DARPA für Schlachtfeld-Kommunikations-Szenarien, kurz darauf begannen Forschungs-Institute und -Unternehmen wie SRI International, sich mit diesem Thema zu befassen. Als Mesh WLAN Hersteller sind sowohl etablierte als auch Start Up Namen zu finden: Accton, BelAir Networks, Cisco, D-Link, FireTide Networks, Intel, InterDigital, Mitre, Motorola / MeshNetworks, NextHop Technologies (Client Adapter), Nokia, Nortel, NTT DoCoMo, PacketHop, Philips, SOHOware, Strix Systems, Swisscom Innovations, Symbol, Thomson, Texas Instruments, Tropos Networks.



weiter auf Seite 18

Zweitthema

Sind SIEM-Tools schon produktiv einsetzbar?

von Dipl.-Inform. Detlef Weidenhammer

Sicherheitsrelevante Informationen werden heute von nahezu sämtlichen IT-Systemen geliefert. Eine schier unüberschaubare Flut von Daten ergießt sich dabei über dem geplagten IT-Personal, bleibt deshalb aber leider auch allzu oft nahezu unbeachtet. Die Gründe dürften in stetiger Arbeitsüberlastung, noch mehr aber im fehlenden Know-how zur Interpretation der Daten liegen. Dabei sind diese übermittelten Informationen äußerst wertvoll, da sie sowohl bei kurzfristigen (Real-Time Monitoring) als auch bei langfristigen Auswertungen (Trend- und Forensik-Analysen) dringend benötigt werden. In diesem Artikel werden die bisherige Entwicklung und der aktuelle Stand der Verarbeitung von Log- und Eventinformationen aufgezeigt.

Brauchbare Informationen zur IT-Sicherheit finden sich heute in nahezu allen Log- und Eventdaten, die von den verschiedensten Systemen aufgezeichnet werden. Hierzu gehören natürlich in erster Linie reine Sicherheitskomponenten wie Firewalls, Content-Filter, Virenscanner oder IDS-Systeme. Aber auch Router, Server, Switches und immer mehr Anwendungssysteme sind bei entsprechender Konfiguration durchaus in der Lage wichtige Informationen zu liefern. Damit fangen aber die eigentlichen Probleme erst an. Der wirklich nutzbringende Umgang mit den gesammelten Sicherheitsinformationen wird auf vielfältige Art und Weise behindert:

weiter auf Seite 9

Aktuelle Kongresse

ComConsult IT-Sicherheits-Forum 2008

ab Seite 7

Geleit

SIP wichtiger als IP?

ab Seite 2

Report des Monats

Neuerscheinung Ende Februar: Siemens HiPath 8000 im Praxistest

ab Seite 16

Zum Geleit

SIP wichtiger als IP?

Das Session Initiation Protocol SIP ist ohne Frage die wichtigste Infrastruktur-Entwicklung seit der Erfindung von IP. Während IP den Transportkern für alle Anwendungsbereiche realisiert, bildet die Kombination aus SIP und IP das Fundament für jede zukünftige Form von Realzeit-Kommunikation:

- Sprache /Telefonie
- Video / Video-Konferenz
- Mehrpunkt-Konferenzen
- Web-Konferenzen / Web-Präsentationen

SIP ist eine Infrastruktur-Komponente, keine Anwendung. Es realisiert und steuert Multimedia-Kommunikations-Verbindungen zwischen einer beliebigen Zahl von Partnern. Um dies leisten zu können, wurde eine völlig neue Architektur geschaffen. Die Intelligenz und vor allem die Medienauswahl liegt im Endsystem, die Vermittlungsinstanz findet die Partner und erstellt Verbindungen.

Mit diesem völlig neuartigen Architektur-Ansatz sind eine Reihe von erheblichen Vorteilen verbunden

- Beliebige Erweiterbarkeit durch neue Dienste/ neue Medien
- Hohe Skalierbarkeit
- Hohe Verfügbarkeit durch einfache und standardisierte Anlagen-Konzepte
- Niedrige Kosten
- Stufenweiser Aufbau möglich, kein Kompletteinstieg erforderlich

Der zentrale Aspekt der Marktbedeutung von SIP ist genau wie bei IP die Nicht-Beschränkung auf ein Unternehmen. SIP liefert eine Infrastruktur, die über Unternehmensgrenzen hinaus geht, die Weltumfassend ist. Mit SIP startet ein völlig neues Kapitel der Kommunikation.

Die Vorteile für Endanwender und Unternehmen liegen auf der Hand:

- Hohe Effizienz in der Kommunikation
- Freie Wahl der Medien in der Kommunikation
- Beliebiger Mix Sprache/Video/Präsentation/Grafik/Daten

SIP wird eine Revolution im Bereich Vertrieb und Support auslösen. Die hier zu realisierenden Potenziale sind kaum abzuschätzen, sie werden in den nächsten Jahren die Welt verändern so wie es IP getan hat.

SIP ist nicht ohne Tücken:

- in der Realität sind die Architekturvarianten vielfältig und schränken die leichte Erweiterbarkeit je nach Hersteller und Produkt deutlich ein

- SIP ist eine Infrastruktur und keine Anwendung, von daher sind die mit SIP kommenden Leistungsmerkmale, obwohl sie umfangreich sind, nicht auf dem Niveau traditioneller Sprachlösungen. Im Endeffekt orientiert sich SIP an Leistungsmerkmalen, die Unternehmensübergreifend Sinn machen. Gleichzeitig bietet SIP den Herstellern aber die Basis für Unternehmensinterne herstellerspezifische Leistungsmerkmale wie die Chef-Sekretärinnen-Funktion, die ja über Unternehmensgrenzen hinaus keine Rolle spielen

Für den Endanwender und die Unternehmen liegt ein erhebliches Problem darin, dass jeder Hersteller vorgibt SIP zu machen, also scheinbar gar keine Unterschiede existieren. Dies ist definitiv falsch.

Eine Studie von ComConsult-Research, die viel Aufsehen erregte, zeigt auf, wo die einzelnen Hersteller zu SIP stehen und worin sie sich unterscheiden (Detaillierte Informationen zur SIP-Studie: „Session Initiation Protocol: Funktionsweise, Einsatzszenarien, Vorteile und Defizite“ finden Sie auf unserer Homepage unter www.comconsult-research.de)

Im Endeffekt lässt sich das Umsetzungsproblem von SIP auf wenige zentrale Frage reduzieren:

- Wie offen ist die Lösung
- Wie leicht kann die Lösung über Unternehmensgrenzenhinweg genutzt werden
- Wie leicht können SIP-Lösungen anderer Hersteller eingebunden werden
- Welche Leistungsmerkmale existieren dabei

Wer diese zentrale Frage nicht berücksichtigt, der wird bei der traditionellen QSIG-Basic-Call-Diskussion enden. Viele Anbieter reduzieren SIP-Leistungsmerkmale zwischen verschiedenen Produkten auf rudimentäre Leistungsmerkmale.

Eine solche Vorgehensweise widerspricht vollständig dem Konzept und dem eigentlichen Ziel und Mehrwert von SIP:

- Offenheit der Lösung
- Unternehmens-übergreifende Kommunikation, direkte Unterstützung von Vertriebs- und Service-Prozessen
- Kompletter Leistungsmerkmal-Umfang auch zwischen verschiedenen Herstellern
- Medien-Freiheit

Die weitere Entwicklung von SIP wird im Wesentlichen von IBM und Microsoft geprägt werden. Diese Hersteller konzentrieren sich auf Kollaborations-Mehrwertdienste. Speziell Microsoft setzt den Markt mit dem OCS stark unter Druck. Viele Großkunden werden die Lizenz zu sehr günstigen Konditionen erhalten (wenn nicht umsonst), damit wird ohne Frage eine breite Basis für dieses Produkt entstehen. Je mehr die Kunden sich an die damit angebotenen Dienste gewöhnen, desto größer wird der Druck auf den Markt. IBM folgt mit den für die folgenden Monate angekündigten Produkten voll dieser Linie. Auch Cisco und Siemens liegen mit ihren Lösungen voll in diesem Trend. Für die Unternehmen besteht hier die Gefahr, dass TK-Lösungen und Kollaboration auseinander laufen und somit wichtige Mehrwerte blockiert werden.

Damit entsteht eine weitere Schlüsselfrage:

- Sind hybride Anlagen-Architekturen mit integrierten SIP-Gateways überhaupt sinnvoll?

Der Vorteil hybrider Anlagen ist klar:

- Gute Migration aus einer bestehenden TK-Welt
- Angebot des vollen Umfangs der traditionellen Leistungsmerkmale
- SIP-Integration über Gateways und Trunks

SIP wichtiger als IP?

Das Problem ist, dass diese Architektur in einigen Bereichen völlig am Ziel vorbei geht:

- Offenheit
- Freie Medienwahl
- Leichte Ausbaubarkeit um neue Medien
- Volle SIP-Leistungsmerkmale zwischen verschiedenen Unternehmen

Die Frage muss gestellt werden, ob hybride Lösungen den Kunden nicht um wichtige Zukunftsperspektiven berauben.

Hier setzt unser top-aktuelles Forum an, das ComConsult SIP-Forum 2008.

Das ComConsult SIP-Forum 2008 analysiert für Sie:

- Was ist SIP?
- Wie sollte eine saubere Basisarchitektur zur Einführung dieses zentralen Infrastruktur-Dienstes aussehen?
- Erfüllen die Hybridlösungen der klassischen TK-Hersteller die Anforderungen an SIP?
- Der große Vergleich: Cisco, IBM, Microsoft, Siemens in der ComConsult-Wettbewerbsanalyse

Dies wird eine brisante und ohne Frage Diskussions-reiche Veranstaltung. Versäumen Sie nicht, sich hier rechtzeitig einen Platz zu sichern.

Zum Ende kommend die Frage: ist SIP also wichtiger als IP? Da es auf IP basiert, sicher nicht. Aber die Auswirkungen auf entscheidende Arbeitsabläufe, auf Effizienz in Prozessen und auf die Art und Weise, in der wir in Zukunft miteinander kommunizieren, sind so weitgehend, dass SIP ohne Frage die wichtigste Infrastruktur-Entwicklung der letzten 10 Jahre ist.

SIP wird in den nächsten Monaten und Jahren noch Anlass zu zahlreichen Diskussionen geben. Viele traditionelle Lösungen werden sich stark ändern müssen, wenn sie im direkten Wettbewerb bestehen wollen. Der Kampf zwischen IT und TK um den wichtigen Kollaborationsmarkt hat gerade erst begonnen. Er wird mit Sicherheit heftig und spannend.

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult SIP- und Unified Communication Forum 2008

Die ComConsult Akademie veranstaltet vom 21. - 22. April 2008 das „ComConsult SIP- und Unified Communication Forum 2008“ in Frankfurt.

SIP ist die wichtigste Infrastruktur-Entwicklung seit der Erfindung von IP. Es realisiert die Kerninfrastruktur für alle zukünftigen Kommunikations-Lösungen von der Sprache über Video bis hin zur Web-Konferenz. Ähnlich wie bei IP bereits geschehen wird SIP die Welt verändern. So extrem wichtige Prozesse wie Vertrieb und Service werden völlig neue Perspektiven erhalten. SIP ist die Basis für Unternehmens-übergreifende multimediale Kommunikation, die eine Effizienz der Kommunikation schaffen wird, die so bisher nicht erreichbar war.

Neue Formen der Kommunikation erfordern neue Architekturen. Diese werden seitens der Hersteller unter dem Begriff „Unified Communication“ eingeführt. Wie der Name Unified bereits ausdrückt, geht es um die Integration aller Kommunikationsdienste in einer gemeinsamen Architektur.

Das ComConsult SIP- und Unified Communication Forum ist eine herausragende Veranstaltung, die zur richtigen Zeit diese wichtige Infrastruktur-Entwicklung aufgreift.

Im einzelnen analysiert das Forum:

- Was ist SIP, was leistet es?
- Wie sieht eine zukunftsorientierte SIP-Architektur aus?
- Unified Communication: was bedeutet das, wo liegen die Knackpunkte
- Kollaboration in der Analyse: was leisten die neuen Dienste, sind sie den Aufwand wert
- TK-Hybridlösungen und SIP/Unified Communication: was geht, was geht nicht
- Die ComConsult-Research Wettbewerbsanalyse: Cisco. IBM, Microsoft, Siemens im Vergleich
- TK-Migration zu SIP: Alternativen, Sackgassen und gute Wege

Ein Kernpunkt des Forums ist die Wettbewerbsanalyse zwischen Cisco, IBM, Microsoft/Nortel und Siemens. In der Auseinandersetzung zwischen den Produkten dieser Hersteller wird der deutsche Markt entschieden. Auch die anderen Hersteller wie Avaya , Alcatel u.a. sind wichtig, aber die Frage über die Akzeptanz der neuen Funktionalität und die Qualität der TK-IT-Integration wird zwischen diesen Herstellern entschieden.

Wir analysieren für Sie auf dem Forum:

- Einsatzerfahrungen und Analysen zu Microsoft OCS
- Praxistest HiPath 8000, Ausblick auf OpenScape 3
- Analyse der neuen IBM-Sametime-Version, was bringt die Zusammenarbeit zwischen IBM und Siemens
- Analyse des Cisco-Produktportfolios: schafft Cisco als einziger Anbieter den Kompromiss zwischen IT und TK

Wie im letzten Jahr planen wir eine Podiumsdiskussion mit marktführenden Herstellern. Viele sehr kontroverse Themen geben die Basis für eine viel versprechende Diskussion.

Versäumen Sie nicht sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern. Profitieren Sie noch bis zum 01.03.08 vom vergünstigten Frühbucher-Preis.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult SIP- und Unified Communication Forum 2008

☐ Ich buche den Kongress
SIP- und Unified Communication Forum 2008
21.04. - 22.04.08 in Frankfurt
zum Preis von € 1.390,- zzgl. MwSt.*
* gültig bis 01.03.08 -
dann € 1.590,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

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

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

Aktueller Kongress

Netzwerk-Redesign Forum 2008

Die ComConsult Akademie veranstaltet vom 14. - 17. April 2008 das „Netzwerk-Redesign Forum 2008“ in Königswinter.

Netzwerke sind der Lebensnerv der IT. Sie unterliegen einer permanenten Weiterentwicklung, wobei sich die Anforderungen nahezu permanent verändern. Parallel verändern sich die Möglichkeiten, die neue Netzwerk-Technologien liefern. Aus diesem Mix aus Bedarf und Potenzial muss das wirtschaftliche und technische Optimum gefunden werden. Da Netzwerke bereits vorhanden sein müssen bevor entsprechende Projekte umgesetzt werden können, muss das Netzwerk-Design grundsätzlich an der Zukunft orientiert sein.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2008 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design und einen stabilen und zuverlässigen Betrieb.

Das ComConsult Netzwerk-Redesign Forum ist traditionell der Treffpunkt der deutschen Netzwerk-Branche. Es bildet die ideale Basis, um sich technisch auf dem Laufenden zu halten und zu sehen, was im Markt passiert.

Die Schwerpunktthemen des ComConsult Netzwerk-Redesign-Forums 2008 sind:

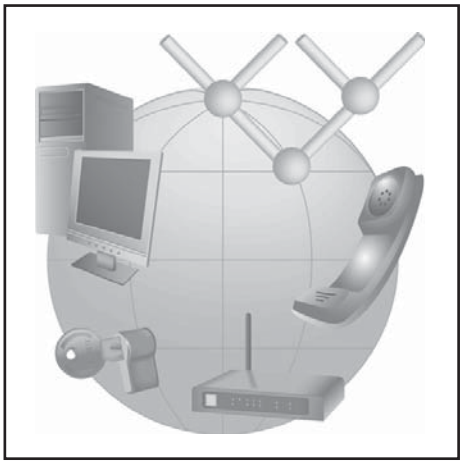
Applikations-bewusste Netzwerke

Netzwerke und Applikationen wachsen weiter zusammen. Dies zeigen die Diskussionen über Web-Technologien, SOA und Kollaboration. Doch was bedeutet das eigentlich? Wir analysieren auf dem Forum

- Wie werden Applikations-bewusste Netzwerke aufgebaut?
- Welche Applikationen sind im Moment wichtig?
- Schwerpunkt: SOA-bewusste Netzwerke in der Analyse

WAN-Redesign

Weiterverkehrs-Konzepte sind im Umbruch. Das zunehmende Angebot von Gigabit Ethernet in Ballungsräumen, der weitere Verfall der Preise, das alles schafft die Basis für neue IT-Architekturen. Wichtige neue Anwendungsbereiche wie SOA basieren auf dieser Weiterentwicklung.



Desaster Recovery bekommt ohne Frage eine neue Dimension.

- Wir geben den Überblick: was passiert im WAN?
- Welche Leistungen entstehen, wie weit kann das gehen?
- Was leisten WAN-Optimizer?

Rechenzentrum und
Server-Konsolidierung

Bereinigung der Server-Vielfalt, Virtualisierung oder nicht, Blade oder nicht, Stromversorgung, Doppelböden und Klimatisierung vor dem Kollabs: RZ- und Server-Konsolidierung ist eines der wichtigsten Themen im Markt. Es ist untrennbar mit der Frage verbunden: wie erfolgt die sinnvolle Einbindung in die Netzwerk-Infrastrukturen

Wir analysieren:

- Was leisten RZ-Netzwerke? Wo liegen Unterschiede zu traditionellen Netzwerken?
- Welche Alternativen gibt es in der physikalischen Realisierung: Komponenten, Standorte, Kabel, Entfernungen?
- Wie kann Verfügbarkeit sicher gestellt werden: die Rolle der verschiedenen Redundanz-Mechanismen?
- Sonderkomponenten in der Analyse: Blade-Switches und ihre Integration, machen sie Sinn
- Load-Balancer

Integration mobiler Mitarbeiter /
Fixed-Mobile-Konvergenz

Einbindung aller relevanten Mitarbeiter in die wichtigen Geschäftsprozesse, egal wo sich diese befinden. Das Thema ist nicht neu, aber die technischen Möglichkeiten verändern sich. Mehr Bandbreite, neue Gerätetechnologien, andere Applikations-Architekturen schaffen die Voraussetzung für mehr Effizienz und Erfolg mobiler Mitarbeiter.

Wir analysieren:

- Fixed-Mobile-Konvergenz: was bedeutet das?
- Wohin geht der weitere Weg? Wie groß sind die Potenziale wirklich?
- Wie gut und nutzbar sind die Produkte?

Video

Wieder einmal wird dem Markt ein massiver Trend Richtung Video vorher gesagt. Dies passiert nicht zum ersten Mal. Ist es diesmal anders? Technisch spricht einiges dafür. Neue Typen von hochqualitativen Desktop-Kameras, Wideband-Sprachcodecs, die Integration in wichtige Applikationen, das alles verändert die technische Landschaft. 2008 wird seitens der Hersteller ein Mega-Video-Jahr werden. Die Tragweite für die Infrastrukturen ist gewaltig.

Wir analysieren

- Was kommt an Video-Produkten? Speziell: was leisten Cisco, Microsoft, IBM und Siemens?
- Wo liegt der Mehrwert?
- Welche Anforderungen stellt dies an die Infrastrukturen?

Voice-over-IP und Kollaboration

Aus der klassischen Sprachkommunikation wird immer mehr eine Mischung aus Sprache, Video und Kollaboration. Reine IP-Telefonie ist tot, sie wird von SIP-basierter Multimedia-Kommunikation abgelöst. IBM und Microsoft mischen 2008 den Markt auf. Speziell Cisco und Siemens versuchen, eine Brücke zwischen den Welten zu schlagen. Fazit ist: Kommunikation ist im Wandel. Die Frage ist nicht ob, sondern wann und wie viele der neuen Funktionen zum Einsatz kommen. Dieses Thema hat erhebliche Auswirkungen auf unsere Infrastrukturen. Fehleinschätzungen in diesem Bereich können schnell zum Kollabs der gesamten Netzwerk-Infrastrukturen führen (adaptive, redundante Codecs auf langsamen WAN-Strecken zum Beispiel).

Netzwerk-Redesign Forum 2008

Wir analysieren:

- Was passiert momentan bei IP-Telefonie und Kollaboration?
- Wie stark prägen IBM und Microsoft den zukünftigen Markt?
- Welche Auswirkungen hat das auf Netzwerke: Bandbreite, Quality of Service, Benutzertrennung, Laufzeiten, Codecs
- Wie sieht ein geeignetes Design aus?

Ethernet in der Produktion

Nahezu unmerklich macht sich Ethernet in der Produktion breit und breiter. In der Standardisierung wird weiter an entsprechenden Redundanz-Verfahren gearbeitet. Die großen Automobilhersteller haben dieses Thema als Muss auf ihren Fahnen stehen.

Wir analysieren:

- Was passiert in der Normung?
- Wo unterscheiden sich Produktionsnetze von „normalen“ Netzwerken?
- Wohin geht der Weg?

Wireless-Netzwerke

Mit IEEE 802.11n erreichen Wireless-Netzwerke ein neues Potenzial. Mit dem von Marvell gerade angekündigten neuen Chip werden Rohdatenraten von 450 Mbit/s möglich (real vermutlich um die 250 maximal). Für Neubauten wird damit eine rein Wireless-basierte Tertiär-Struktur möglich. Parallel haben alle Hersteller ihre Produktlinien überarbeitet. Wireless-Switches bieten erhebliches Potenzial für den Betrieb und neue Anwendungen. Und damit nicht genug: mit MESH-Netzwerken kommen neue Möglichkeiten hinzu.

Wir analysieren:

- Was passiert zurzeit bei Wireless-Technologien, wohin geht der Weg?
- Was leistet 802.11n? Als Ersatz für Kabel-gebundene Netzwerke geeignet?
- Was leisten Wireless-Switches? Wo unterscheiden sich die Produkte? Zeit für einen Standard, wo steht CAPWAP?
- Ist MESH die Zukunft? Ist dies mehr als eine Wireless-Technologie, ist dies die Basis für eine neue Art von Kommunikations-Architektur?

Sicherheit

Je mehr Anwendungen in Netzwerken realisiert werden, umso größer wird der Bedarf an Sicherheit. Dies umfasst sowohl die Kontrolle des Zugangs zu wichtigen Servern, Applikationen und Daten als auch die Verhinderung einer gegenseitigen Beeinflussung von Applikationen im Netzwerk. In keinem Fall darf ein Fehlverhalten einer Applikation oder eines Benutzers andere Applikationen oder Benutzer stören. Die technologischen Ansätze im Bereich Sicherheit sind weit reichend und vielfältig, aber zum Teil Hersteller-gebunden und inkompatibel. Wie kann man hier zu einer sinnvollen und noch beherrschbaren Lösung kommen?

Wir analysieren:

- Was bietet der Markt?
- Wie können Benutzer- und Applikationstrennung realisiert werden?
- NAC, 802.1x und ähnliche Technologien: wie kann in diesem Wald aus Hersteller-spezifischen und zum Teil nicht kompatiblen Lösungen ein sinnvoller und angemessener Weg gefunden werden, der nicht zum Overkill wird?
- Wo geht der Markt hin? Haben wir weiteren Bedarf oder sollte das jetzt angebotene Portfolio gepflegt und bereinigt werden?

Das ComConsult Netzwerk-Redesign Forum 2008 ist die zentrale Netzwerk-Veranstaltung des Jahres 2008. Sie ist für jeden Entscheider, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung!

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2008

Ich buche den Kongress
Netzwerk-Redesign Forum 2008
14.04. - 17.04.08 in Königswinter

☐ mit Intensiv-Training am letzten Tag zum Preis von € 2.190,- zzgl. MwSt.

☐ ohne Intensiv-Training am letzten Tag zum Preis von € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer vom_____bis_____08

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

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

Kongress

ComConsult IT-Sicherheits-Forum 2008

Die ComConsult Akademie veranstaltet in Zusammenarbeit mit der der GAI NetConsult vom 26. - 29. Mai 2008 ihr diesjähriges „IT-Sicherheits-Forum 2008“ in Frankfurt.

Das IT-Sicherheits-Forum wird auch in diesem Jahr wieder einen umfassenden Überblick zu aktuellen Themen der IT-Sicherheit in Theorie und Praxis anbieten. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und neutralen Fachvorträgen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf sofort verwendbare Informationen gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können. Das Gesamtprogramm umfasst den bewährten Ablauf:

- Aufzeigen aktueller Trends bei Bedrohungen und Schutzmaßnahmen
- Vorstellung und Bewertung neuer Sicherheitstechnologien
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- „Best Practice“ Sessions mit Sicherheitsempfehlungen für den Tagesbetrieb
- Tutorien und Seminare für Anfänger und Fortgeschrittene

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und auch Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese in Vor- und Nachmittagssitzungen parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als Themen des IT-Sicherheits-Forums 2008 sind bisher u.a. vorgesehen:

- Sind SIEM-Tools schon produktiv einsetzbar?
  - Security Information and Event Management - Aktueller Stand
  - Log-Management, Security-Operations, Compliance-Reports
  - Empfehlungen zur Produktauswahl
  - Fehler, die bei einer SIEM-Einführung zu vermeiden sind

- Database Security
  - Status und typische Probleme

  - Trends bei SQL-Injection
  - Bewertung der Oracle Transparent Database Encryption (TDE)
  - Hinweise zur Verbesserung der Database-Security

- IT-Sicherheit in Virtualisierungsumgebungen
  - Wie gut sind virtuelle Maschinen abzusichern
  - VM unterschiedlichen Sicherheitsniveaus auf dem gleichen Server
  - Welche zusätzlichen Schutzmaßnahmen sind zu treffen?
  - Wann schließt sich der Einsatz von VM aus?

- SAN-Security
  - SAN-Technologien und ihre Sicherheitsschwächen
  - Session-Hijacking, DoS und Man-in-the-Middle-Angriffe
  - SAN-Design unter Sicherheitsaspekten

- Physische Sicherheit in IT-Umgebungen
  - Haftungsrisiken für IT-Verantwortliche
  - Sicherheit in der Bauausführung und Infrastruktur
  - Sichere Ausführung von Energieversorgung, Zugangs- und Brandmeldetechnik • Technische Sicherheit der IT-Komponenten

- Storm Worm - ein Beispiel für neue Internet-Gefahren
  - Entstehen und aktuelle Gefährdungslage des Storm Worm
  - Technische Analyse
  - Kommunikation des P2P-Netzwerkes
  - Vorbereitung auf zu erwartende Aktivitäten

- Einschätzungen zu Standards im Sicherheitsbereich
  - BSI- und / oder Internationale Standards
  - Sicherheitsmanagement nach ISO 2700x
  - Best Practices für Notfallplanung
  - Welche Kombinationen von Standards haben sich durchgesetzt?

- Business Continuity Management
  - Sicherung kritische Geschäftsprozesse bei Störungen oder Notfällen
  - Best Practice Prozesse nach ITIL, BCI und DRII
  - Vorgehensmodell: BIA, Strategie, Implementierung, Pläne, Tests
  - Empfehlungen zum Tooleinsatz

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

- Welche Bedrohungen erwarten uns in 2008?
- Sicherheitsempfehlungen zum SAP-Betrieb
- Sicherheitsmaßnahmen beim Einsatz von USB-Sticks und Speicherkarten
- Erstellung und Betrieb von sicheren Webanwendungen
- Erhöhte Anfälligkeit der IP-Infrastruktur
- Content-Security: Spyware wird immer gefährlicher

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat seinen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden auch neue Entwicklungen aufgezeigt, die sowohl Informationen zu Bedrohungen, als auch zu Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in die Geschäftsabläufe, da hier noch immer die größten Defizite anzutreffen sind. Damit bietet das IT Sicherheits-Forum für Sicherheitsverantwortliche, aber auch für vorrangig technisch interessierte Teilnehmer eine Fülle wertvoller Informationen.

IT-Sicherheits-Forum 2008

10% Frühbucherrabatt bis 31.03.08

IT-Sicherheits-Forum 2008

26.05. - 29.05.08 in Frankfurt a.M.

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das IT-Sicherheits-Forum 2008 bis zum 31.03.2008 für eine rabattierte Teilnahmegebühr an.

IT-Sicherheits-Forum 2008 inkl. Tutorium am ersten Tag
zum Preis bei Buchung bis 31.03.08 von € 1.590,-
statt regulär € 1.790,- zzg. MwSt.

IT-Sicherheits-Forum 2008 ohne Tutorium am ersten Tag
zum Preis bei Buchung bis 31.03.08 von € 1.990,-
statt regulär € 2.190,- zzg. MwSt.

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult
IT-Sicherheits-Forum 2008

Ich buche den Kongress
ComConsult
IT-Sicherheits-Forum 2008
26.05.08 - 29.05.08 in Frankfurt a.M.
☐ mit Tutorium am ersten Tag
zum Preis von € 1.990,- zzgl. MwSt.*
☐ ohne Tutorium am ersten Tag
zum Preis von € 1.590,- zzgl. MwSt.*

* gültig bis 31.03.08
(dann reguläre Preise € 2.190,- bzw. 1.790,-zzgl. MwSt.

Bitte reservieren Sie für mich
ein Hotelzimmer

vom_____bis_____08

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

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

Zweitthema

Sind SIEM-Tools schon produktiv einsetzbar?

Fortsetzung von Seite 1

Dipl.-Inform. Detlef Weidenhammer ist seit 1994 Geschäftsführer der GAI NetConsult GmbH und hat seitdem in einer Vielzahl von Projekten national und international agierende Unternehmen bei der Konzeption von Netzwerk- und Sicherheitslösungen unterstützt. Seine fachlichen Schwerpunkte liegen in den Bereichen IT Risk Management, Security-Auditing und Security Management. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen auch als Verfasser von Publikationen und als Referent bei Seminaren und Kongressen ein. Er leitet das jährlich stattfindende „IT-Sicherheits-Forum“ und ist Herausgeber der Fachpublikation „Security Journal“.

- Immense Datenflut führt schnell zur Missachtung
  Abhängig von der Konfiguration liegt das Volumen der gesammelten Daten schon bei kleinen IT-Umgebungen sehr schnell im Gigabyte-Bereich. Bei großen Unternehmen kann man mit einer Flut von hunderten Millionen Events pro Tag rechnen. Dabei kann man sich leicht vorstellen, dass die Administratoren allein mit der Bewältigung dieser Datenflut völlig überfordert sind. Nicht selten führt dies dazu, dass die Daten ohne Auswertung einfach gelöscht werden.

- Wirklich interessante Daten gehen leicht unter
  Ein Großteil der gesammelten Daten ist aus Sicherheitssicht bestenfalls als „Hintergrundrauschen“ zu bezeichnen. So liefern selbst bei guter Kalibrierung Sicherheitskomponenten wie IDS oder Firewalls nur ca. 10% bis 20% wirklich interessante Daten, der Rest ist zumeist verzichtbar. Bei der Eventauswertung von Servern, Desktops oder Applikationen ist der interessante Anteil sogar deutlich unter 10% anzusiedeln. Berücksichtigt man nur noch Events, die zu Alarmen führen, dann dürfte diese Rate unter 1% liegen. Umso wichtiger, dass sie nicht im allgemeinen Rauschen untergehen.

- Datenauswertung überfordert das Personal
  Soll die Auswertung der gesammelten Informationen aus Sicherheitssicht relevante Ergebnisse liefern, ist auch Fachpersonal mit sehr gutem Sicherheits-Knowhow erforderlich, um Fehlalarme zu erkennen oder Zusammenhänge zwischen anscheinend unabhängigen Events herzustellen. Wenn überhaupt vorhanden, ist dieses Personal aber in den meisten Unternehmen wohl eher mit anderen Arbeiten beschäftigt.

- Keine Beachtung des „Business Impact“
  Die gesammelten Informationen sind ihrer Herkunft nach eher technischen Einzelproblemen zuzuordnen und werden zudem ohne Bewertung ihres Einflusses auf Geschäftsabläufe (business impact) behandelt. Hierzu wäre z.B. die Kenntnis und Beachtung von Schutzbedarfswerten und Risikoeinstufungen notwendig.

- Nicht standardisierte Datenformate erschweren die Auswertung
  Neben dem verbreiteten Formaten (syslog, SNMP-Trap) verwendet nahezu jeder Hersteller ein eigenes Format bei der Erzeugung seiner Logdaten bzw. Event-Informationen. Dies erschwert deutlich die Auswertung und auch die vergleichende Bewertung der Daten.

- Fehlende Event-Korrelation führt schnell zu Datenwirrwarr
  Daten, die aus verschiedenen Quellen stammen, beschreiben häufig nur verschiedene Stufen eines Angriffs oder sind sogar dem gleichen auslösenden Ereignis zuzuordnen und könnten dann deutlich reduziert werden. Angriffe, die den gleichen Verursacher besitzen, sich aber gegen verschiedene Ziele richten, werden heute zumeist unabhängig voneinander behandelt. Wesentliche Erkenntnisse gehen dabei verloren.

Um die o.g. Problembereiche auch nur annähernd in den Griff zu bekommen, sind intelligente Tools gefragt. Diese sollten idealerweise wertvolles menschliches Personal teilweise ersetzen können, aber auch Funktionen zur schnelleren Reaktion auf Sicherheitsvorfälle enthalten.

Ist SIEM die lang erwartete Lösung?

SIEM, das „Security Information and Event Management“, ist die sinnvolle Weiterentwicklung der vor wenigen Jahren aufgetauchten SIM (Security Information Management) und SEM (Security Event Management) Toolsets. Während SEM vorrangig Ereignisse sammelt und in Realzeit darstellt, ist SIM in der Tradition altbekannter Loganalyzer mit der umfassenden Sammlung der im Netzwerk gesammelten Logdaten betraut, fügt aber als Neuerung bei seinen Auswertungen eine gewisse Sicherheitsintelligenz hinzu. So können z.B. proaktiv Alarme generiert, Sicherheitsmaßnahmen wie Patches vorgeschlagen oder die Zuordnung zu bewerteten Business-Risiken vorgenommen werden. Auch die Verifikation von potentiellen Schwachstellen durch integrierte Vulnerability-Scanner zum Abgleich mit Angriffsversuchen stellt einen weiteren interessanten Fortschritt dar. Das Zusammenwachsen der beiden Ansätze SEM und SIM führt nun zum integrierenden SIEM mit den bisher schon gewohnten Bestandteilen Collect, Normalize, Enrich, Correlate, Report und Archive.

Ein wesentlicher Treiber dieser neuen Entwicklung ist in der Erfüllung von Compliance-Anforderungen z.B. von SOX, HIPAA oder Basel-II zu sehen. Unternehmen sind zunehmend gezwungen, die Beachtung nationaler und internationaler Regularien für ihre Business-Prozesse und IT-Anwendungen nachzuweisen, wobei unterstützende Tools natürlich stark gefragt sind. Diese Super-Tools versprechen damit also die eierlegende Wollmilchsau zur Verarbeitung aller Sicherheitsinformationen zu werden. Wollen wir doch nachstehend

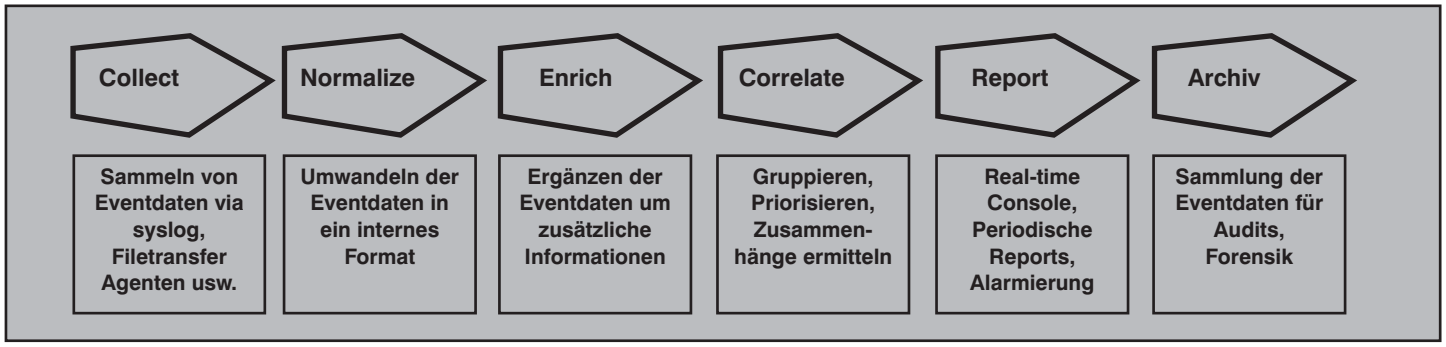


Abbildung 1: Der SIEM-Prozess

analysieren, was von diesem Versprechen zu halten ist.

Topologie einer SIEM-Lösung

Eine typische SIEM-Lösung besteht aus den event-liefernden Netzwerk-Komponenten und dem eigentlichen SIEM-Tool mit dem Event-Collector, der Core-Engine, den SIEM-Applications, den Funktionen des User-Interfaces und der zugehörigen Datenbank. Bei den meisten SIEM-Lösungen können einzelne Teile aus Performance- oder Verfügbarkeitsgründen auch auf weitere Systeme (zumeist Appliances) ausgelagert werden.

Netzwerk-Komponenten wie Firewalls, Content-Gateways, IDS-Systeme, Router, Server, Switches, usw. registrieren Events und können diese auf die unterschiedlichsten Arten weitergeben. Man unterscheidet je nach Art der Datensammlung SIEM-Tools mit eigenen Agenten auf den Netzwerk-Komponenten („agent-oriented“) von denen, die „agentless“ arbeiten. Spezialisierte SIEM-Agenten haben den Vorteil, dass sie gleich eine Vorverarbeitung der Rohdaten „vor-Ort“ vornehmen können. Damit lässt sich das zu transferierende Datenvolumen deutlich verringern und das eigentliche SIEM-System entlasten. Nachteil ist jedoch, dass jegliche Vorverarbeitung einen Informations- und Kontextverlust zur Folge haben kann und spätere Auswertungen nie mehr auf die unverfälschten Rohdaten zurückgreifen können.

Einen Typ „agentless“ gibt es streng genommen gar nicht, da immer ein Stück Software auf dem event-liefernden System

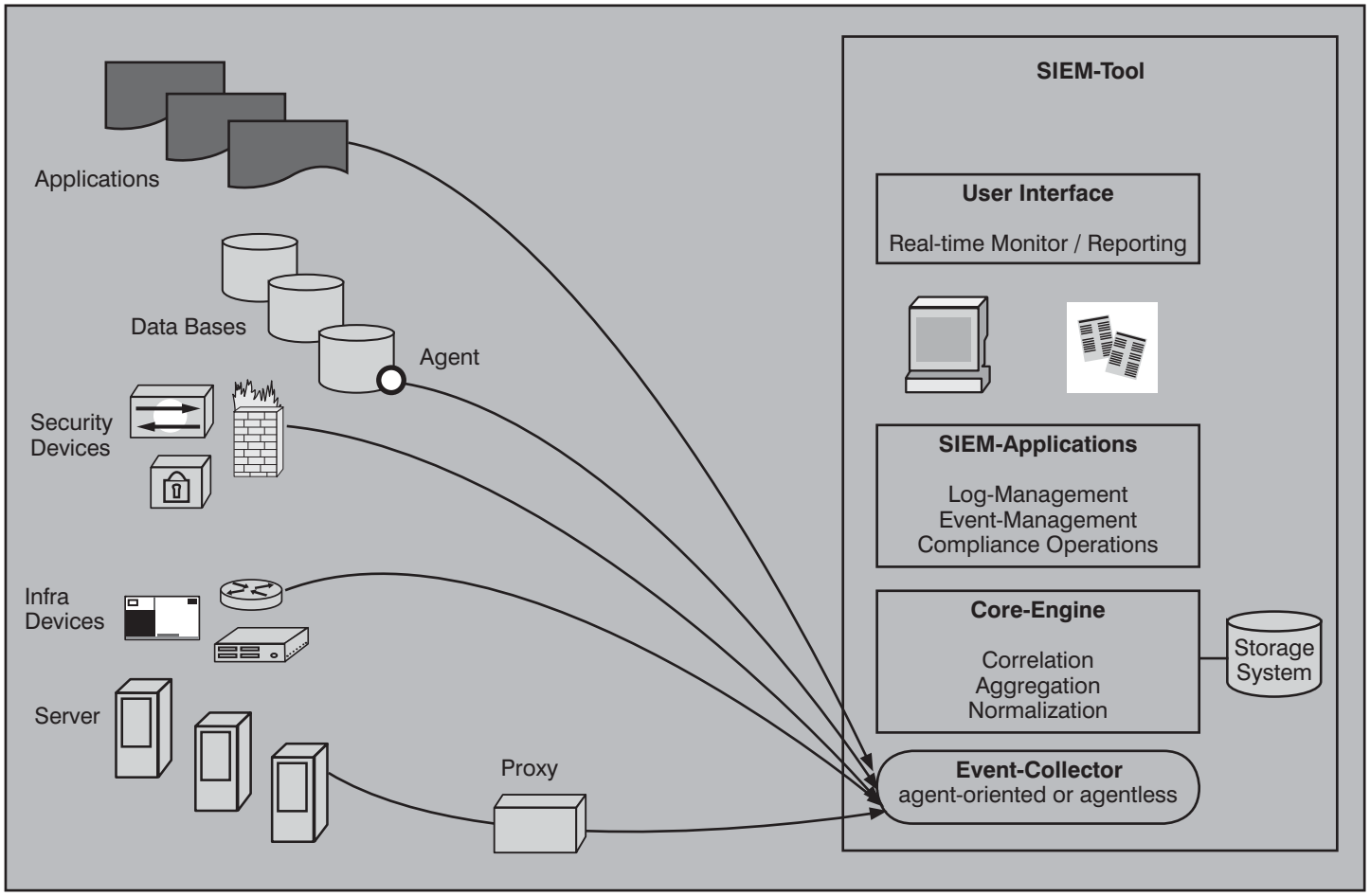


Abbildung 2: Komponenten einer SIEM-Lösung

implementiert sein muss, das in der Lage ist, die gewünschten Daten zu liefern. Gemeint ist in diesem Zusammenhang, dass allein Standardmöglichkeiten der Netzwerk-Komponenten hierzu genutzt werden. Darunter ist in erster Linie die Verwendung der allgemein anzutreffenden syslog und SNMP-Traps zu verstehen. Bei SIEM-Lösungen, die den Typ „agentless“ propagieren, ist zu berücksichtigen, dass damit aber auch Nachteile verbunden sind. Die höhere Last auf Netzwerk und Zentralsystem wurde bereits erwähnt, hinzu kommen die fehlenden Möglichkeiten sicher festzustellen, ob wirklich alle Events weitergeleitet wurden. Eine Spielart dieser zwei Grundvarianten stellen sog. Proxy-Agents dar, die die Rohdaten empfangen und nach einer Vorverarbeitung an das SIEM-System weitersenden. Häufig findet man aber auch Mischformen dieser Ansätze, um alle Möglichkeiten in einer Lösung abzudecken. Idealerweise entscheidet der Nutzer dann selber darüber, welchen Ansatz er bevorzugt.

Über einen sicheren Kanal, wenn das genutzte Transportprotokoll dieses hergibt, werden die Daten dann zum Event-Collector auf dem SIEM-System direkt oder über einen Proxy-Agenten transferiert.

Core-Engine mit den Basisfunktionen

Um die vorliegenden Daten weiter verarbeiten zu können, müssen sie zunächst in eine vergleichbare Form gebracht werden. Solch eine **Normalisierung** ist durchaus problematisch wegen der immer noch fehlenden Standardisierung der Datenformate und -inhalte von Logs/Events. Anpassungen durch sog. Connectoren für die verbreiteten syslog, SNMP Traps, ODBC sind zwar weit verbreitet, reichen aber bei weitem noch nicht aus. Gebraucht werden z.B. auch Snort syslog, Snort Database, Check-Point OPSEC, PIX over syslog, CISCO router over syslog usw. Über jede spezifische Eventquelle muss also das SIEM-System Kenntnis haben, um die einlaufenden Eventdaten weiter bearbeiten zu können. Die meisten SIEM-Tools besitzen zwar ein SDK (Software Development Kit), damit der Betreiber selber Connectoren für nicht von Hause aus unterstützte Systeme schreiben kann, doch wer hat dafür schon Zeit?

Was passiert aber, wenn sich das Datenformat bei einem Hersteller-Update plötzlich ändert? Man wird evtl. einige Zeit darauf warten müssen, bis das Connector-Update vorliegt, in dieser Zeit können die Rohdaten aber nicht verarbeitet werden und die Überwachung ist zumindest unvollständig. Genau diese Problematik trifft heute bereits bei IDS-Systemen zu, die vom jeweiligen Hersteller mit einem steten Fluss von Vulnerability-Pattern versorgt werden und somit dem Kenntnisstand der SIEM-Lösung immer deutlich voraus sind. Das führt dann dazu, dass solche (unbekannten) Events dann zumeist gar nicht bis zur Auswertung gelangen.

Ein möglicher Ausweg aus dieser Problematik könnte die im letzten Jahr von der MITRE Corp. (auch verantwortlich für CVE, CME, usw.) vorgestellte Common Event Expression (CEE) sein. Diese standardisiert unter Nutzung einer allgemeinen Sprache und Syntax, wie Eventdaten beschrieben, geloggt und ausgetauscht werden können. Es ist zu hoffen, dass sich möglichst viele Hersteller an dieser Entwicklung beteiligen.

An die Normalisierung schließt sich dann die **Aggregierung** an, bei der die Daten durch Weglassen von redundanten Informationen (z.B. bei tausenden von Events durch einen Portscan) verdichtet werden.

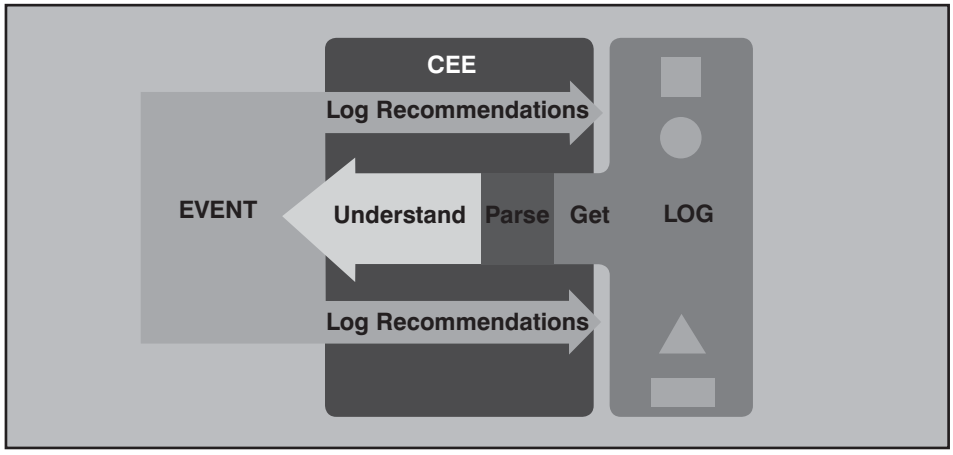


Abbildung 3: MITRE CEE für Event-Interoperabilität

Kern jeder besseren SIEM-Lösung ist die **Korrelation**, die die Aufgabe hat, alle einlaufenden Events zu analysieren und Anzeichen für gerade stattfindende Angriffe festzustellen. Realzeitanforderungen sind hierbei natürlich besonders wichtig, da man möglichst schnell reagieren muss. Dies stellt aber besondere Anforderungen an eine höchst performante Bearbeitung im SIEM-System, die eigentlich nur durch rein memory-basierte Operationen leistbar ist. Langdauernde Database-Zugriffe würden den Zeitanforderungen nicht gerecht werden.

Typischerweise werden für die Korrelation Regel- und Statistik-basierte Techniken eingesetzt. Regelbasierte Korrelation nutzt vorgegebene oder selbst erstellte Regeln, um nach spezifischen Events zu suchen. Dies können z.B. Würmer, Viren, Buffer Overflows oder DDOS-Angriffe sein. Bei der statistikbasierten Korrelation werden Events in zuvor bestimmte Angriffskategorien eingeordnet und eine potentielle Angriffswahrscheinlichkeit berechnet. Können bei der Korrelation auch noch spezifische Bewertungsgrößen für die IT-Umgebung und die „business assets“ berücksichtigt werden, sind Angriffe gegen kritische Unternehmensbereiche schneller erkennbar.

Das **Storage System** schließlich sammelt die Event-Daten zur späteren Auswertung, z.B. um Langzeitanalysen oder forensische Untersuchungen durchzuführen. Zum Einsatz kommen SQL-basierte Datenbanken oder eine eigene File-orientierte Ablage. Wichtig zu klären ist, ob die ausgewählte SIEM-Lösung nicht nur die endbehandelten Daten speichert, sondern auch die Rohdaten. Dies ist zu empfehlen, da damit mögliche Informationsverluste durch die Core-Engine weitgehend ausgeschlossen werden.

SIEM-Applications

Das **Log-Management** kann wohl als einer der Ursprünge von SIEM gelten und stellt auch heute noch eine Kernfunktion dar. Kaum ein Administrator kann die Unmengen der anfallenden Logdaten bewältigen. Das Volumen der gesammelten Daten kann schon bei kleinen IT-Umgebungen täglich sehr schnell im Gigabyte-Bereich liegen. Dabei kann man sich leicht vorstellen, dass die Administratoren allein mit der Bewältigung dieser Flut an Daten überfordert sind. Soll die Auswertung der gesammelten Informationen aus Sicherheitssicht relevante Ergebnisse liefern, ist darüber hinaus Fachpersonal mit sehr gutem Sicherheits-Knowhow erforderlich. Dieses ist bekanntlich eine knap-

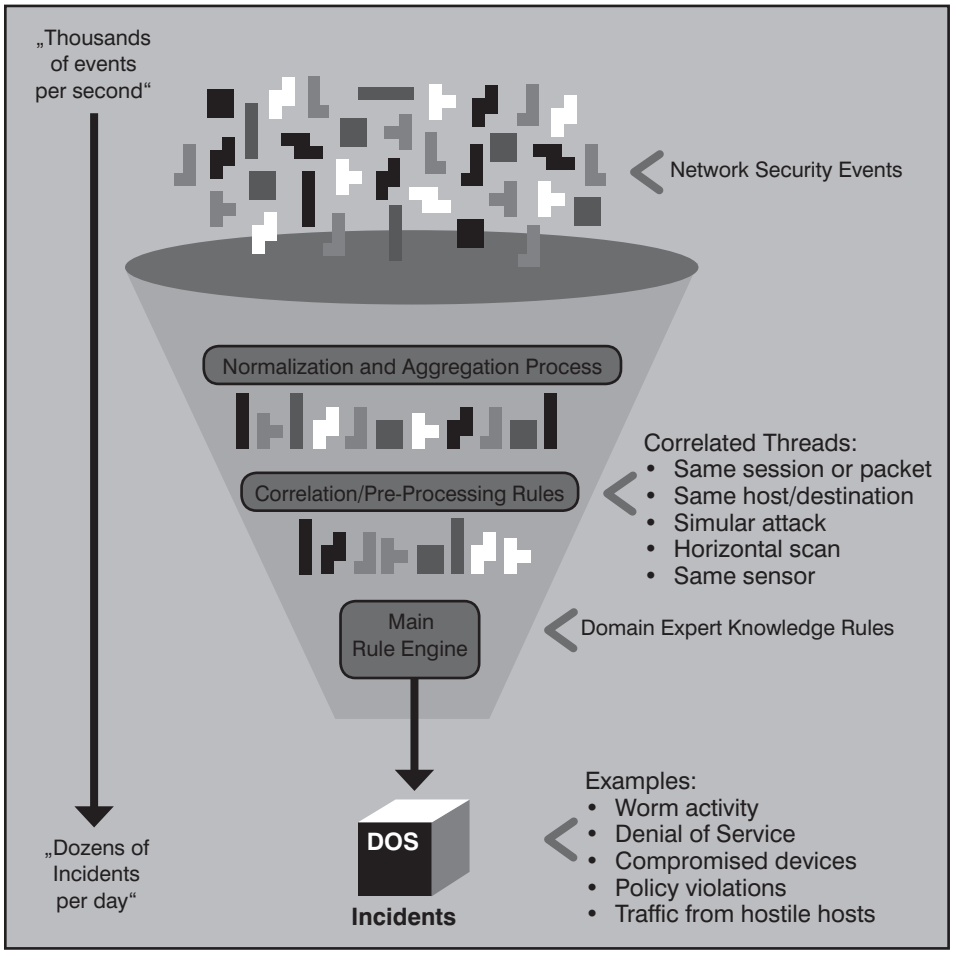


Abbildung 4: Reduktion der Datenflut (Quelle : High Tower Software)

pe Ressource und wird bestimmt nicht vorrangig mit der Sichtung von Logdaten beschäftigt sein. Allein das Log-Management durch effiziente Tools zu unterstützen, würde sich also bereits lohnend auswirken.

Das **Event-Management** liefert den notwendigen Mehrwert durch zusätzliche Sicherheitsanalysen, weshalb SIEM-Lösungen auch nicht mit den einfacheren Log-Analyzern auf eine Stufe zu stellen sind. Durch die Aggregierung der Events wird das Datenvolumen deutlich verringert und durch die Korrelation werden Zusammenhänge zwischen einzelnen Sicherheitsvorfällen aufgedeckt. Im besten Fall kann man den gesamten Angriffsweg verfolgen und entsprechend reagieren. Die gesammelten Informationen sind ihrer Herkunft nach auch eher technischen Einzelproblemen zuzuordnen und werden auch meistens gleichrangig behandelt. Eine weitergehende Korrelation mit den übergeordneten Zusammenhängen eines Business-orientierten Risk Managements und der Möglichkeit zur Priorisierung waren bisher kaum möglich, da eine Verbindung zwischen Technik- und Business-Daten zumeist nicht gegeben ist.
Das alles sind zumindest die Aussagen der Hersteller. In der Realität ist aber gerade das Gebiet der „event-correlation“ noch eher ein interessantes Forschungsthema als in Produkte gegossene Realität. Die meisten SIEM-Systeme sind heute kaum in der Lage, die einfachsten Korrelationen herzustellen, wie sollte man da erwarten können, dass damit der Einsatz teuren Personals eingespart werden könnte. Trotzdem macht der eingeschlagene Weg Mut, fast jeder SIEM-Hersteller liefert vorgefertigt hunderte von Korrelationsregeln mit und über Regel-Editoren lassen sich eigene Erweiterungen hinzufügen.

Compliance Reports

Eine wesentliche Triebfeder zur Weiterentwicklung von SIEM-Lösungen sind die Comliance-Anforderungen, die viele Unternehmen heute zu erfüllen haben. Ob SOX, HIPAA, PCI, Basel-II oder wie sie alle heißen mögen, je nach Standort und Unternehmenstyp sind heute eine Vielzahl von Richtlinien zu erfüllen. Die alleinige Überwachung der Perimeter-Security reicht dafür nicht aus, noch viel wichtiger ist die Überwachung aller Events innerhalb des eigenen Netzwerkes, denn hier werden sensible Firmeninformationen erzeugt, gelesen, modifiziert und gespeichert. Ein Monitoring-System muss deshalb in der Lage sein, eine hohe Eventlast zu verarbeiten und Nutzer- und Systemaktivitäten in allen Abschnitten einer Session zu verfolgen. Dazu gehört insbesondere auch die ständige Bereitstellung von Überwachungsmöglichkeiten z.B. für:

- Access Management (Benutzerzugriffe, unautorisierte Zugriffe)
- Configuration Management (Datenänderungen, Konfigurationsänderungen)
- Malware-Detection (Anomalien, Ausführung von Malware)
- User Management (Nutzerprivilegien, Nutzerrichtlinien)

Von einigen SIEM-Lösungen wird hierfür bereits eine Vielzahl von vorgefertigten Reportmustern bereitgestellt. So wertvoll diese Auswertemöglichkeiten auf den ersten Blick auch erscheinen mögen, so vorsichtig sollte man an deren Nutzung herangehen. Die Reports sind nach unseren Erfahrungen nicht immer sachgerecht erstellt (falsche Bezüge auf Standards oder Richtlinien) und decken oft auch nur einen kleinen Teil der insgesamt erforderlichen Unterlagen zu Compliance-Prüfungen ab. Immerhin ist damit aber ein Weg zu aussagekräftigen Reports aufgezeigt, die Lösungen werden hier sicherlich noch an Qualität gewinnen. Mit etwas Aufwand ist sogar die Erstellung eigener Reports möglich, die dann natürlich bestens auf die eigenen Belange hin angepasst werden können.

User Interface

Reporting und Visualisierung sind die äußerlich sichtbaren Erfolgsfaktoren einer jeden SIEM-Lösung. Das Reporting umfasst zumeist bereits eine Vielzahl von vorgefertigten Standardformaten, die auf Techniker, aber auch auf das Management zugeschnitten sind. Die Visualisierung muss in graphischer Form auf sich anbahnende Angriffe hinweisen, sollte vielfältige Darstellungsmöglichkeiten bis zum Zoom auf Ereignisebene bieten und unbedingt über einen Real-Time Monitor verfügen.

Marktübersicht

Plant man die Einführung einer SIEM-Lösung, dann sollte man zunächst klären, für welche Kernaufgaben (reines Log-Management, Handling von Security-Events, Compliance-Reports, oder alles zusammen) diese eigentlich vorgesehen ist. Es gibt weltweit eine Vielzahl von Lösungen,

Abbildung 5: Realtime-Monitor (Quelle: RSA/enVision)

die sich das Label SIEM gegeben haben und deren Funktionsumfang und Reifegrad deutliche Unterschiede aufweist. Nachstehend sollen einige derjenigen genannt werden, die auch in Deutschland über eine nennenswerte Basis an Installationen verfügen.

Umfassende SIEM-Lösungen mit dem Schwerpunkt Log-Management und Compliance-Reporting kommen von RSA/enVision, Symantec und Q1 Labs. Solche mit starkem Fokus auf Security und Event-Management kommen von ArcSight, Intellitactics und netForensics. Unter den Herstellern finden sich auch einige große Namen, die ihre bereits vorhandenen Lösungen z.B. zum Netzmanagement durch SIEM-Funktionen erweitert haben: IBM, Computer Associates, NetIQ.

Auswahl einer SIM-Lösung

Ist der Kreis der Anbieter gemäß obiger Kategorisierung auf eine übersichtliche Anzahl eingeschränkt, dann sollte auch unbedingt eine Einschätzung derselben bzgl. Kundenbasis und Service in Deutschland beinhalten, bevor man sich auf die Technik stürzt. Einige kritische Fragen sind möglichst bereits vorab zu klären:

- Wie sollen Logging und Datentransport behandelt werden?
  Es ist genau zu klären, welche Sicherheitsinformationen geliefert werden. Kommt nur SYSLOG in Frage oder sind auch andere Formate gefragt? Soll der Datentransport gesichert werden, dann sind die hierfür bestehenden Möglichkeiten zu klären. Bei SNMPv1 wären hierfür zusätzliche Maßnahmen vorzusehen.

- Abschätzung des Datenaufkommens und der EPS (Events-per-Second)
  Zur Festlegung der Testausstattung sind halbwegs realistische Angaben über das zu erwartende Datenaufkommen zu machen. Insbesondere bei der Nutzung von WAN-Verbindungen ist darauf zu achten, dass diese nicht zu sehr belastet werden.

- Aufbewahrung von Daten
  Gibt es Aufbewahrungsfristen für Log- und Eventdaten, die zu beachten sind? Welches Datenvolumen muss dann aufbewahrt werden? Sind die geplanten Speichermöglichkeiten dafür ausreichend oder muss in Richtung NAS/SAN erweitert werden?

- Sind besondere Fähigkeiten des Personals einzuplanen?
  Wenn das zu testende SIEM-Produkt hohe Anforderungen an die Datenbank-Administration stellt, ist dies entsprechend einzuplanen. Um eine einführende SIEM-Schulung wird man in der Regel nicht herumkommen.

Nach erfolgter Vorauswahl sollten ein oder mehrere Produkte In-house mit der vorhandenen IT-Umgebung intensiv getestet werden. Es gilt dabei, die vom Hersteller zugesicherten Funktionsumfänge genauestens zu überprüfen. Häufig beschreibt gerade in diesem noch recht jungen Fachgebiet die Paperware nicht unbedingt die wirklichen Möglichkeiten der Hard/Software. SIEM-Lösungen stellen darüber hinaus auch hohe Ansprüche an die interne Organisation und Vorbereitung. Auf dem SANS Log Management Summit formulierte Tom Chmielarski von Motorola hierzu aus eigener Erfahrung die “Top 5 Mistakes and Misconceptions”. Gravierende Fehler seiner Meinung nach waren:

1. Die Erwartung mit der reinen Installation von SIEM überhaupt ein Problem zu lösen
2. Keine Ahnung über die mit SIEM lösbaren Probleme zu haben
3. Das Versäumnis vorher realistische Nutzungsszenarien aufzustellen
4. Das Versagen die verfügbaren Daten überhaupt zu verstehen
5. Das Versagen SIEM dem Business schmackhaft zu machen

Wie man daraus ersieht: die gute Vorplanung spielt eine immens wichtige Rolle bei der Einführung einer SIEM-Lösung.

Einführung einer SIEM-Lösung

Die Einführung einer SIEM-Lösung, die nicht nur zum einfachen Sammeln und Anzeigen von Logdaten dienen soll, sondern durch hochwertige Anwendungen einen wirklichen Mehrwert für die Betreiber bietet, erfordert besondere Sorgfalt. Ein Stufenplan sollte bereits vor der technischen Installation folgende Abschnitte abarbeiten:

- Vorbereitungen
  Vor der Einführung der technischen Komponenten sollte man sich zunächst einen vollständigen Überblick über die eigene IT-Landschaft verschaffen. Man sollte hierfür sogar in Erwägung ziehen, einen externen Auditor zu beauftragen, um eine möglichst objektive Bewertung zu erlangen. Hierzu gehören auch die Ermittlung von aktuellen Schwachstellen und die Identifikation von potentiellen Schwachstellen. Weiterhin sind sämtliche relevanten IT-Objekte und Funktionen zu erfassen und in Bezug auf ihre Wertigkeit mit einem relativen oder absoluten Wert zu versehen.

Ziele: Zunächst einmal sollten die eigenen Prioritäten verstanden und geordnet werden, um für später auftretende Fragen gerüstet zu sein. Diese könnten sein: Welche Bereiche gehören zur kritischen Infrastruktur, die später durch das SIEM-System besonders zu überwachen ist? Welche

Sind SIEM-Tools schon produktiv einsetzbar?

Funktion	Bedeutung
Basis-Architektur	
Gut skalierbare Hardware	Ermöglicht spätere Upgrademöglichkeiten bei steigenden Ansprüchen
Skalierbare Architektur mit multiplen Correlation- und Database-Servern	Ermöglicht Lastverteilung und spätere Erweiterungen. Auch High-Availability sollte möglich sein
Umfangreiche Liste unterstützter Systeme (Datenquellen)	Es sollten möglichst alle vorhandenen Sicherheits- und sonstigen IT-Systeme unterstützt werden, z.B. Firewalls, IDS, Router, Server, Switches usw.
Vielzahl von Integrationsmethoden	Integration weiterer Systeme durch Nutzung von Log Files, ODBC, SNMP, OPSEC usw.
Software Development Kit	Ermöglicht die eigene Erstellung von Agenten oder Connectoren
Funktionen zur Incident Response	z.B. Stoppen von Angriffen durch Information oder Re-Konfiguration von Sicherheitskomponenten
Sichere Übermittlung der Eventdaten	Sichert Vertraulichkeit und Integrität
Überwachung aller SIEM-Komponenten	Alarm bei Ausfall einzelner Komponenten
Granulare Zugriffskontrolle	Zuweisung rollengerechter Privilegien
Updates automatisierbar über Internet	Vereinfachung der Verteilung von Updates und Pattern
Eigenes Case Management oder hierfür Anbindung an externen Systeme	Ermöglicht die zeitgenaue Verfolgung eines Vorfalls durch unterschiedliche Bearbeiter
Vielfältige Möglichkeiten der Alarmierung (Email, SNMP, SMS)	Erleichtert die Einbindung in ein (vorhandenes) Alarmhandling
Event-Management	
Kategorisierung von Events	Aufstellung von herstellerunabhängigen Event-Kategorien
Welche Identifier für Events/Vulns. werden verwendet?	z.B. CVE, BugTraqID,…
Update der Event-Formate	Automatisiertes Update wie bei Virenpattern ist zu fordern
Aufbewahrung der Rohdaten	Neben den normalisierten Daten sollten auch die Rohdaten archiviert werden, um keinen Informationsverlust bei späteren Auswertungen zu haben
Aggregierung von Events	Reduzierung des Datenaufkommens; Zusammenfassung ähnlicher Events (z.B. bei Portscans)
Priorisierung von Events	Einheitliches Gewichtungsschema sollte vorliegen
Integration von Vulnerability Scannern	Ermöglicht eine spezifische Bedrohungsanalyse und Korrelation (ist das Ziel überhaupt verwundbar?), hilft Fehlalarme zu vermeiden
Einfache Regelerstellung	Personal sollte keine Programmierkenntnisse benötigen
Zuordnung von Events zu Vorfällen	Erleichtert die Übersicht
Integration von fremden Knowledge bases	Erleichtert die Analyse eines Events
Security-Management	
Event-Korrelation	Welche Möglichkeiten gibt es? Gibt es vorgefertigte Regelsätze?
Regel-Editor	Können Regeln selbst erstellt werden?
Korrelation in Echtzeit?	Sinnvoll nur bei ausschließlicher Memory-Nutzung
User-Aktivitäten	Können diese verfolgt werden?
Database	
Datenbank mit guter Performance und Skalierbarkeit	Unbedingt notwendig bei hohem Eventaufkommen
Einfaches Datenbank-Management	Fachwissen sollte nicht erforderlich sein
Visualisierung	
Graphisches GUI	Nice-to-have, vereinfacht aber dem Anwender die Übersicht
GUI mit Darstellung korrelierter Events	Vereinfacht die Übersicht
GUI mit anpassbarem Layout	Personalisierung der Darstellung
Darstellung von aktuellen und historischen Events	Erleichtert forensische Untersuchungen
Reporting	
Vielfältige Standard-Reports	Zur Arbeitsvereinfachung und nutzbar als Vorlagen, welche gibt es? Welche Ausgabeformate?
Compliance-Reports	Welche gibt es?
Konfigurierbare Reports	Erstellung eigener Report-Layouts
Automatisierte Reportgenerierung	Erstellung periodischer Reports

Tabelle 1: SIEM-Auswahlkriterien

Alarmstufen sind dafür zu vergeben? Ist die eingestellte Detailtiefe des Loggings sinnvoll bzw. angemessen?

- Vereinfachungen
  „Keep it simple“ sollte zumindest am Anfang auch eine Grundregel der SIEM-Einführung sein. Hierzu sollte man sich zunächst auf die (vorher identifizierten) wichtigsten Objekte konzentrieren, alles andere kostet unnötigen Aufwand und Geld und könnte das Projekt gefährden. Mit den Ergebnissen des ersten Schrittes können evtl. auch Vereinfachungen der IT-Infrastruktur oder der Zugriffsmöglichkeiten der Nutzer vorgenommen werden.

Ziele: Die Einführung einer SIEM-Lösung könnte willkommener Anlass sein, einmal wieder über die Sinnhaftigkeit vergangener Entscheidungen zur IT-Infrastruktur nachzudenken. Sind Vereinfachungen ohne Funktionsverlust zu erzielen, sollten diese umgesetzt werden.

- Tuning
  Mit den Erkenntnissen der beiden ersten Schritte lassen sich weitere Optimierungen vornehmen, insbesondere gilt dies für die wichtige Verarbeitungsgröße Events-per-second (EPS). So liefern IDS-Sensoren je nach Einstellung eine beträchtliche Menge an Daten, die das SIEM zu verarbeiten hat, deshalb sind sie bei Tuningmaßnahmen besonders zu beachten.

Ziele: Durch sinnvolles Tuning an den richtigen Stellen lässt sich viel Geld sparen (Kosten für Hardware, Lizenzen auf EPS-Basis, Betreuung). Dieser Prozess ist auch später im Betrieb in gewissen Abständen zu wiederholen.

Fazit

SIEM hat durch die immer wichtiger werdenden Compliance-Anforderungen bei den Herstellern und auch bei vielen Unternehmen einen neuen Schub erhalten. Das einfache Sammeln und Auswerten von Eventdaten ist mittlerweile kein Problem mehr, wenn man von der Update-Problematik bei IDS-Systemen einmal absieht. Hier wird erst eine Standardisierung der Eventdatenformate eine wirkliche Verbesserung bringen. Problematischer sieht es immer noch bei dem avisierten Einfließen von Security-KnowHow in SIEM-Lösungen aus. Die Korrelation von Events ist noch nicht zufriedenstellend gelöst und gerade die genannte Problematik bei IDS-Systemen stellt eine arge Behinderung dar, da nicht immer alle gemeldeten Events erfasst werden können.

Die Compliance-Reports müssen sehr oft noch als die ersten Versuche der Hersteller auf diesem Gebiet bewertet werden, zu auffällig sind Unsauberkeiten bei der Zusammenstellung der Daten und den Bezügen zu bestimmten Regelwerken. Eine schnelle Besserung sollte hier aber zu erwarten sein, solange muss man sich eben mit eigenen Reports behelfen.

Die am Markt verfügbaren SIEM-Lösungen sind in Preis und Leistung noch sehr unterschiedlich, deshalb sind eine gute Vorauswahl und eine anschließende Evaluierung in Realumgebung unbedingt notwendig. Der Betrieb wird zunächst keine Einsparungen an Personal bringen, es ist eher vom Gegenteil auszugehen, wenn man das Thema ernsthaft betreibt.

Die Zielsetzungen sind klar zu definieren, wobei sinnvollerweise zunächst mit überschaubarem Scope gearbeitet werden sollte. Später kann man die Möglichkeiten der SIEM-Lösung dann auch weitergehend ausnutzen.

Die eingangs gestellte Frage „Sind SIEM-Tools schon produktiv einsetzbar?“ lässt sich also nicht eindeutig beantworten, da dies sehr abhängig ist von den Zielsetzungen des jeweiligen Unternehmens. Lässt sich die Frage beim Schwerpunkt Log-Management noch durchaus bejahen, so sind die Erwartungen an das Security-Management und die Compliance-Reports besser nicht zu hoch zu schrauben. Alles in allem bleibt das Thema SIEM aber weiterhin spannend.

Report des Monats

Siemens HiPath 8000 im Praxistest

Im März erscheint der brandaktuelle Report „Siemens HiPath 8000 im Praxistest“ von ComConsult Research.

Mit der HiPath 8000 hat die Siemens Enterprise Communication nicht nur ein neues Produkt auf den Markt gebracht. Angesichts der Tragweite des zukünftigen SIP-Marktes ist es das zentrale Produkt, das über die Zukunft von Siemens EN entscheiden wird.

Der Report analysiert, wo die HiPath 8000 momentan steht. Die Architektur wird beschrieben und insbesondere der Grad der Offenheit, d.h. die Einhaltung des SIP-Standards untersucht. Die HiPath 8000 wurde zusammen mit Telefonen mehrerer Hersteller getestet, so dass auch ein direkter Vergleich zwischen den OpenStage-Telefonen und den SIP-Telefonen anderer Hersteller entstand. Dies wurde kombiniert mit der Bewertung der Akzeptanz durch den Benutzer. SIP ist anders als traditionelle TK, was sich auch in der Handhabung der Telefone zeigt. Auf der anderen Seite ist eines der großen Versprechen von moderner Telefonie die einfachere Handhabbarkeit der Leistungsmerkmale. Wir analysieren, wie sich die HiPath 8000 aus der Sicht des Endbenutzers darstellt. Abschließend bewerten wir die Anlage aus der Sicht des Betreibers. Wie aufwendig sind insbesondere die täglichen Change-Konfigurationen, wie leicht ist die Anlage in ihrer Konfiguration zu verstehen.

Dieser Report kann sicher einen eigenen Test der HiPath 8000 unter den spezifischen Kriterien Ihres Unternehmens nicht ersetzen. Aber er ist ein wichtiger Baustein in der Evaluierung der Einsetzbarkeit der HiPath 8000 und sollte auf keinem Schreibtisch eines Entscheiders, Planers oder Betreibers fehlen.

Der Autor dieses Reports ist Markus Geller. Er verfügt über langjährige Erfahrung in Forschung, Entwicklung und Betrieb von Lokalen Netzen, IP-TV, Wireless Local Area Networks sowie Sicherheits-Technologien. Als Mitarbeiter der ComConsult Technologie Information GmbH ist er verantwortlich für Produkttests und Marktbeobachtung. Zu diesen Themengebieten ist er zudem als Referent bei der ComConsult Akademie tätig.

REPORTS

Weitere Report-Neuerscheinungen von ComConsult Research

Office Communications Server 2007
In dem vorliegenden Report analysiert ComConsult Research die aktuelle Unified Communications Strategie von Microsoft, in deren Mittelpunkt der Office Communications Server steht.

Sicherheitsmechanismen für Voice over IP
Der Technologie-Report von ComConsult Research stellt - gestützt auf die Erfahrungen aus zahlreichen Projekten sowie Analysen und Tests im ComConsult-Multivendor-Labor - die möglichen und sinnvollen Sicherheitsmechanismen für VoIP ausführlich und im Detail dar und bewertet die vorgestellten Lösungen eingehend hinsichtlich Machbarkeit, Aufwand und Nutzen.

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

Fax-Antwort an ComConsult 02408/955-399

Bestellung

☐ Ich bestelle den Report
„Siemens HiPath 8000 im Praxistest“
zum Preis von € 398,- zzgl. MwSt. und Versand

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Aktuelle Inhouse-Schulung

Voice over IP für TK-ler
Grundlagen, Voraussetzungen, Veränderungen

Die Einführung von Voice over IP (VoIP) ist inzwischen in jedem größeren und sogar schon in vielen mittleren Unternehmen ein Thema geworden. Alle großen TK-Hersteller haben ihre Produktpalette bereits auf VoIP umgestellt und kündigen den Support für konventionelle TK-Anlagen ab. Nicht selten sind aber die bisher mit der Telekommunikationstechnik betrauten Mitarbeiter eines Unternehmens noch nicht auf diese neue Technologie vorbereitet.

Dieser Workshop richtet sich ausschließlich an Mitarbeiter von Unternehmen und Behörden, die bisher mit dem Betrieb konventioneller TK-Lösungen befasst waren und jetzt auf VoIP umsteigen wollen. Dabei wird nicht so sehr auf die tiefgründigen technischen Details der neuen Technologie eingegangen, sondern auf die täglichen Anforderungen - bei der Einführung und beim laufenden Betrieb.

Folgenden Themenschwerpunkte sind im Rahmen des Workshops vorgesehen:

- Grundidee und Basiskonzepte von IP-Telefonie
  - Grundlegende Funktionsweise eines IP-Netzes
  - Welche Unterschiede bestehen zwischen konventioneller und VoIP-Telefonie?
  - Welche Voraussetzungen gibt es für die Einführung von VoIP?
  - Wo liegen die Vor- und Nachteile?
  - Welche Gefahren bringt VoIP mit sich?

- Voraussetzungen an die Infrastruktur
  - Verkabelung, Steckertypen etc.
  - Funktionsweise der Netzwerk-Komponenten
  - Mögliche Fehlerquellen
  - Stromversorgung der Endgeräte
  - Was tun, wenn nur konventionelle Verkabelung vorhanden ist?

- Planungsgrundlagen und Migrationsmöglichkeiten
  - Welche Bereiche des Unternehmens sind VoIP-Ready?
  - Wo sind ggf. Investitionen in die Infrastruktur erforderlich?
  - Was ist bei Kernsanierungen und Neubauten zu beachten?
  - Wie kann eine Umstellung auf VoIP möglichst reibungslos erfolgen?

- Change-Management
  - Wie werden die Endgeräte konfiguriert?
  - Was ist bei Umzügen zu beachten?
  - Was muss der Benutzer bei der Umstellung auf VoIP beachten?

- Fehlerquellen und Notfall-Szenarien
  - Stromausfälle
  - Fehlende Anschlussmöglichkeiten für neue Endgeräte
  - Redundanz-Mechanismen
  - Trouble-Shooting

- Hersteller und Lösungen
  - Welche Arten von TK-Anlagen gibt es (konventionelle, hybride, Softswitch)?
  - Welche Arten von Endgeräten gibt es?
  - Welche Leistungsmerkmale bieten die Endgeräte?
  - Wie unterscheiden sich die Hersteller?

- Wie sieht die Zukunft aus?
  - Welche neuen Leistungsmerkmale sind zu erwarten?
  - Wie müssen sich der Support und das Help-Desk darauf einstellen?
  - Welche Schwierigkeiten sind künftig zu erwarten?
  - Welche Arbeiten fallen weg, welche kommen hinzu?

Zielgruppe
Es sind keinerlei Vorkenntnisse im Hinblick auf IP-Technologien oder VoIP erforderlich, da sich das Seminar an Mitarbeiter eines Unternehmens richtet, die bisher noch nicht mit VoIP oder IP-Netzen in Berührung gekommen sind. Ziel ist es, diese Mitarbeiter für den Umgang mit der neuen Technik fit zu machen, indem Schwellenängste genommen und ein Grundverständnis für VoIP vermittelt wird. Nicht selten sind diese Mitarbeiter sonst sehr schnell von der Entwicklung abgehängt und nicht mehr bereit, sich auf die neuen Anforderungen einzustellen.

Konzept
Um auf die spezifischen Anforderungen einzugehen, findet im Vorfeld der Schulung ein qualifiziertes Vorgespräch statt, anhand dessen die bestehenden und angestrebten Lösungen in einem Unternehmen ermittelt werden, um eine möglichst weit reichende Fokussierung zu ermöglichen. Die enge Abstimmung mit den Verantwortlichen des Unternehmens gewährleistet eine ideale Ausrichtung der Workshop-Inhalte. Die Mitarbeiter des Unternehmens werden so auf die spezifischen Anforderungen vorbereitet und bekommen klare Konzepte an die Hand.

Die Veranstaltung hat den Charakter eines Workshops, um den Teilnehmern einen breiten Raum für individuelle Fragen zu geben und die Diskussion unterschiedlicher Lösungen, Möglichkeiten und Varianten zu erleichtern. Damit werden unterschiedliche Kenntnisstände angeglichen und alle Teilnehmer können einen maximalen Lernerfolg erzielen.

Um die Thematik zu veranschaulichen, verwenden unsere Referenten ein umfangreiches Showcase bestehend aus unterschiedlichen VoIP-Endgeräten, Telefonieservern und Messgeräten bzw. Analysetools. Sie sind eingeladen, damit selbst zu experimentieren!

Die Dauer ist auf zwei Tage angelegt. Wenn gewünscht, kann zum Abschluss des Workshops auch eine Testat durchgeführt werden, um den Kenntnisstand zu überprüfen.

Sollten Sie Interesse an dieser Inhouse-Schulung haben, sprechen Sie uns bitte an. Wir erstellen Ihnen gerne ein individuelles Angebot.

Ihre Ansprechpartnerin bei der ComConsult Akademie: Frau Stephanie Braun

Schwerpunktthema

Vermaschte Wireless Netze: Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s - Teil 1

Fortsetzung von Seite 1

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

Laut State-of-the-Market Report vom Oktober 2007 (Webtorials / Kubernan) setzen 23 Prozent der WLAN Anwender Mesh Technologien ein (siehe Abbildung 1.2).

1.1 Ersatz des Ethernet Distribution Systems

Wireless LAN's bestehen in der Praxis (wie auch im IEEE Basis-Standard beschrieben) nicht nur aus Access Points und gegebenenfalls einem zentralen Controller, sondern auch aus einem Distribution System, das die einzelnen BSS, d.h. Access Points zu einem gemeinsamen ESS verbindet. Das Distribution System ist landläufig ein Layer-2/Layer-3-Ethernet und erfordert somit eine erkleckliche Menge an

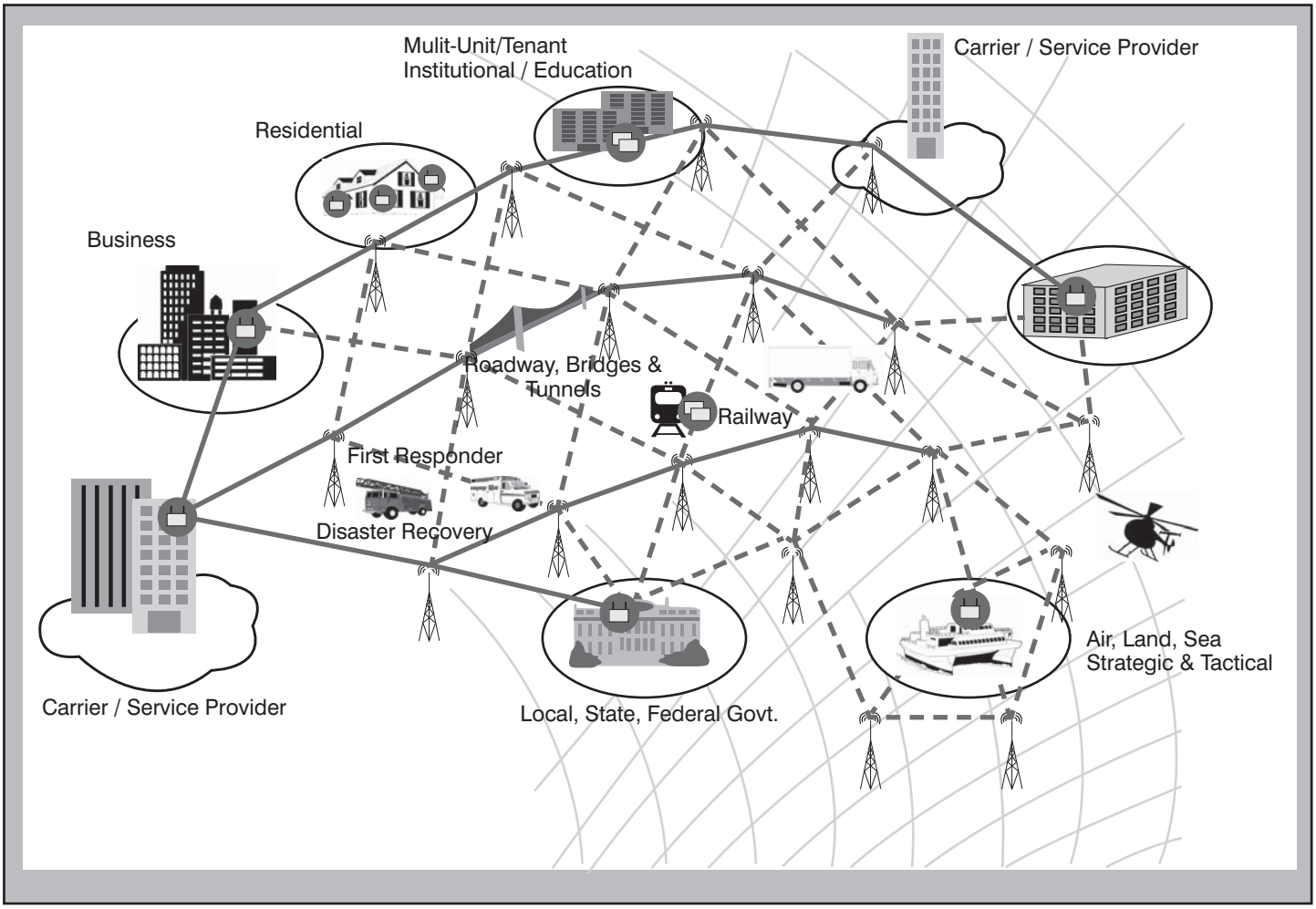


Abbildung 1.1: Vermaschte Wireless Netze

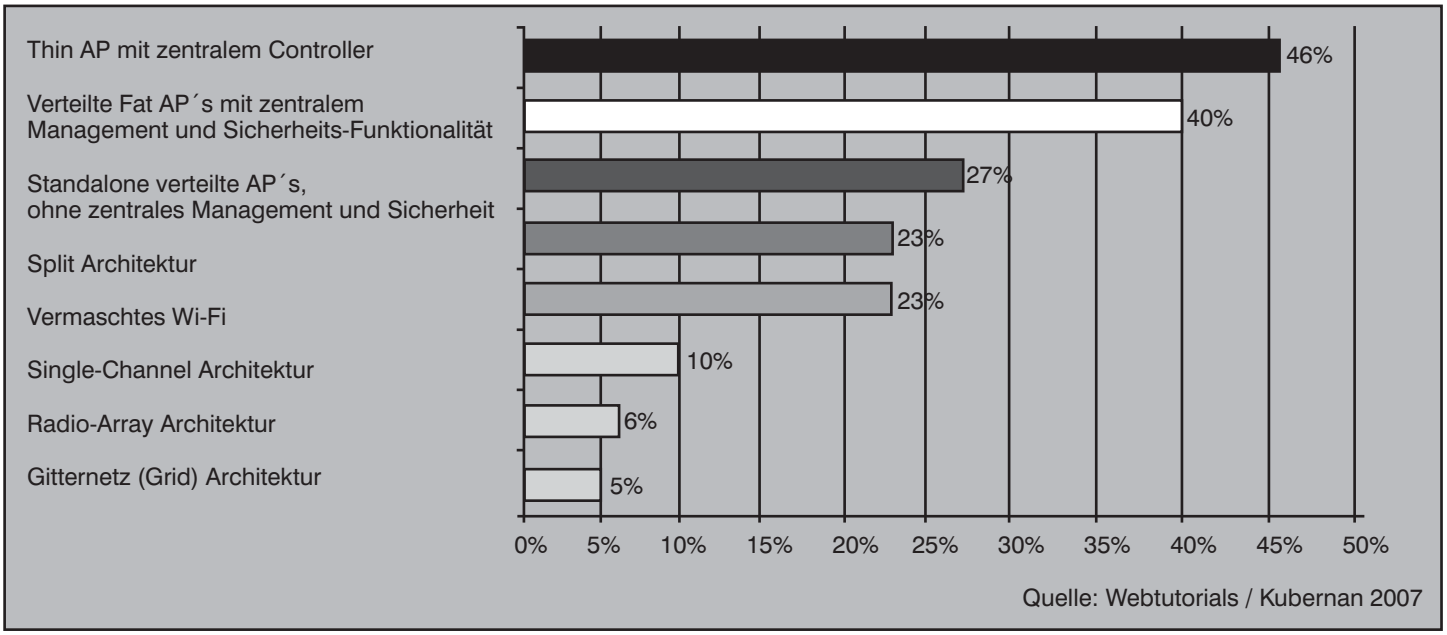


Abbildung 1.2: Verbreitung verschiedener WLAN-Architekturen

drahtgebundenen Anschlüssen, nämlich für jeden einzelnen Access Point mindestens einen Ethernet-Anschluss, bei redundanter Anbindung auch an zwei Ethernet-Anschlüsse. Da Access Points meistens an Stellen montiert werden (nämlich Wand, Decke oder Zwischendecke), an denen keine Verkabelungsdose / Bodentank verfügbar ist, muss vielfach für die Installation einer WLAN-Infrastruktur entsprechend nachverkabelt werden. Das verursacht zusätzliche Kosten und ist bei ad-hoc Netzen d.h. kurzfristigen und vorübergehenden Vernetzungen wie Medien-Events oder Katastrophenfällen gar nicht möglich. Eine Zielsetzung vermaschter WLAN‘s ist es daher, den Verkabelungsbedarf so weit wie möglich zu minimieren und erweiterte Flexibilität in Form von Mobilität und ad-hoc Einrichtung mobiler Netzwerke so weit wie möglich zu maximieren. Die logische Konsequenz ist eine Vernetzung der Access Points mittels Funkverbindungen anstelle der Ethernet-Ankopplung(en). Aus dem Ethernet Distribution System wird so ein Wireless Distribution System mit Funktverbindungen (siehe Abbildung 1.3).

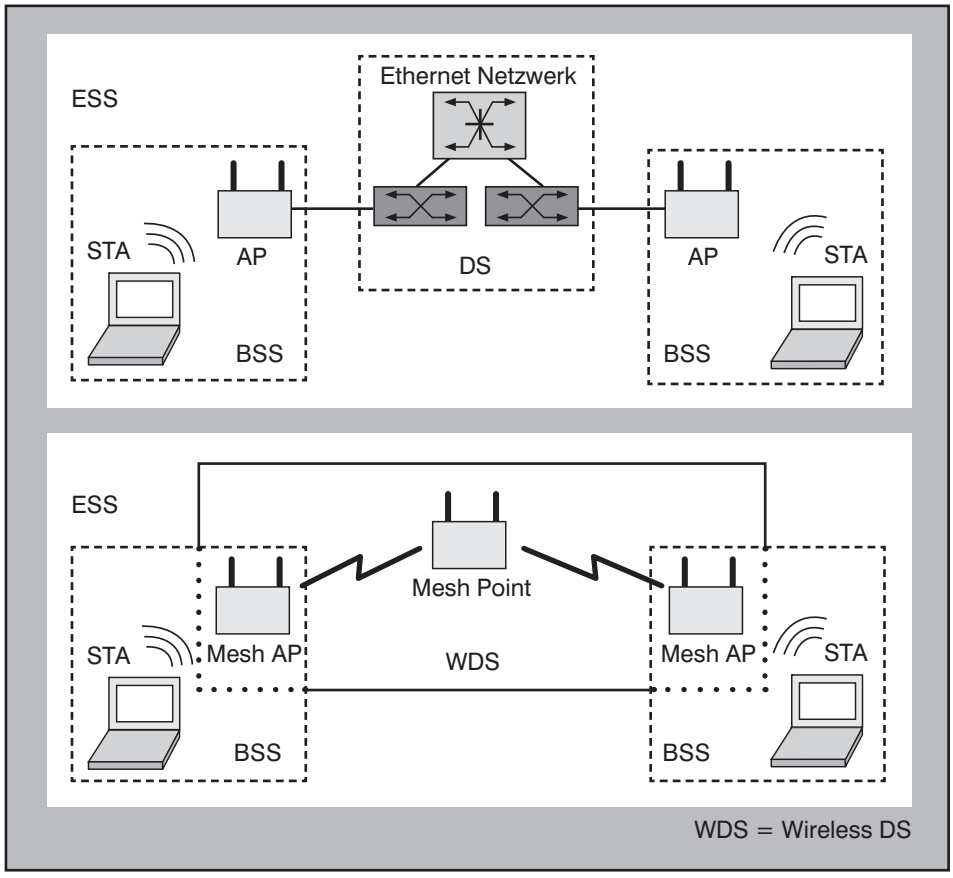


Abbildung 1.3: Vom Ethernet zum Wireless Distribution System

Einfach auf den Punkt gebracht, nutzen vermaschte WLAN‘s eine Topologie mit vermaschten Funkverbindungen zwischen den einzelnen Knoten, um ein selbstkonfigurierendes, fehlertolerantes d.h. „selbstheilendes“ Netzwerk zu bilden (siehe Abbildung 1.4). Da nur einige wenige vermaschte Knoten mit einer Kabel-Anbindung (Ethernet) ausgestattet werden, entfällt einerseits der Bedarf für aufwändige Backbone-Verkabelungen, andererseits werden die Vorteile von optimierter Routenfindung, Lastverteilung und automatischer Fehlerumschaltung auf alternative / Backup Wege erreicht, die zentrale Management-Kontrolle bleibt als Vorteil erhalten. Die Standard-Architektur besteht aus einem reinen „Peer-Netzwerk“ intelligenter vermaschter Knoten, die gleichberechtigt untereinander Informationen austauschen. Als CAPWAP- oder Hersteller-Erweiterung könnten zentrale Controller als Steuerinstanz zum Einsatz kommen.

1.2 Mesh WLAN Typen

Nicht alle Mesh WLAN's sind gleich aufgebaut, einige wenige Lösungen schließen die Clients als vermaschte Knoten mit ein, die meisten Lösungen schließen sie aus. Vermaschte WLAN's lassen sich in verschiedene Typen unterteilen:

- Infrastruktur Mesh WLAN
- Client Mesh
- Mix Mesh WLAN:

In einem **Infrastruktur Mesh** WLAN sind nur Access Points / Mesh Komponenten und Portale (Übergang in andere Netze), jedoch keine Clients integriert. Alle Komponenten haben Mesh Routing Intelligenz. Mesh Komponenten (Mesh Points, manchmal auch WLAN Router genannt), Mesh Access Points und Mesh Portale leiten als fest positionierte Netzkomponenten mit einer Sendeleistung von 100mW bis 800mW den Verkehr zwischen Endgeräten oder zwischen einem Endgerät und dem verkabelten Netzwerk weiter. Clientsysteme sind reine Sender-/Empfängersysteme und von jeder Weiterleitungs-Funktionalität ausgeschlossen (z.B. Accton, BelAir, Cisco, FireTide, Strix, Symbol, Tropos). Infrastruktur Mesh Lösungen zielen vielfach mehr auf den Outdoor als den Indoor Markt. Im Vergleich zu WLAN Switching verlagert ein Infrastruktur Mesh Netzwerk Routing und Load Balancing Intelligenz in die Mesh Knoten, behält aber die zentrale Kontroll- und Management-Instanz bei.

In einem reinen **„Client Mesh** WLAN", agiert jedes (gleichzeitig mobile) Endgerät inklusive Laptops, PDA's und Softphones als Weiterleitungs-Komponente (Relay) für andere Endgeräte, d.h. die Daten eines Benutzers / Endsystems durchlaufen die aktuell benachbarten Endgeräte und „Wireless Router" als „Hop", um ihren Zielpartner – gegebenenfalls auch im verkabelten Netzwerk – per Transit über das Funknetz hinweg zu erreichen. Die Sendeleistung beträgt z.B. 200mW, die Reichweite 500m bis 800m für IEEE 802.11b (z.B. NextHop). Die vernetzten Clientsysteme bilden dabei ein vermaschtes Netzwerk, das automatisch „um Leistungsengpässe und Hindernisse herum" routet. Zu beachten ist jedoch: Soweit der Routing Algorithmus auf Peer-to-Peer Kommunikation fokussiert ist, findet keine Optimierung der Client-Server Verbindungswege statt (!).

Bei **Mix Mesh** WLAN bilden Mesh Komponenten, Access Points und Portale den Kern des vermaschten WLAN Netzwerks und haben daher volle Mesh Routing Intelligenz. Clients haben nur eine deutlich reduzierte Mesh Routing Funktionalität (Nachbar-Erkennung, Kommunikation mit benachbarten Clients / Knoten). Eine typische Einschränkung ist hier, dass Clients nur ihre direkte Nachbarn sehen, nicht jedoch die gesamte Topologie des vermaschten WLAN's kennen, wie dies bei Mesh Routern oder Access Points der Fall ist. Clientsysteme werden als eingeschränkt intelligente Mesh Knoten insbesondere zur flexiblen Erweiterung des vermaschten WLAN's genutzt, insbesondere hinsichtlich Ausdehnung (z.B. MeshNetworks, PacketHop).

Die aktive Teilnahme der Clients an der Frame-Weiterleitung („Routing") hat den Vorteil, dass Handoff / Reassoziierung wegfallen, da der Client sozusagen sein eigener Router / Access Point ist. Zudem argumentieren die Hersteller von Client Mesh Netzen, dass durch die Integration der Clients als Relay-Komponenten das Problem „Reichweite vs. Abdeckung / Datenrate" entschärft wird. Cient Mesh Lösungen zielen wegen der insgesamt deutlich niedrigeren Leistung dabei mehr auf den Indoor als den Outdoor Markt.

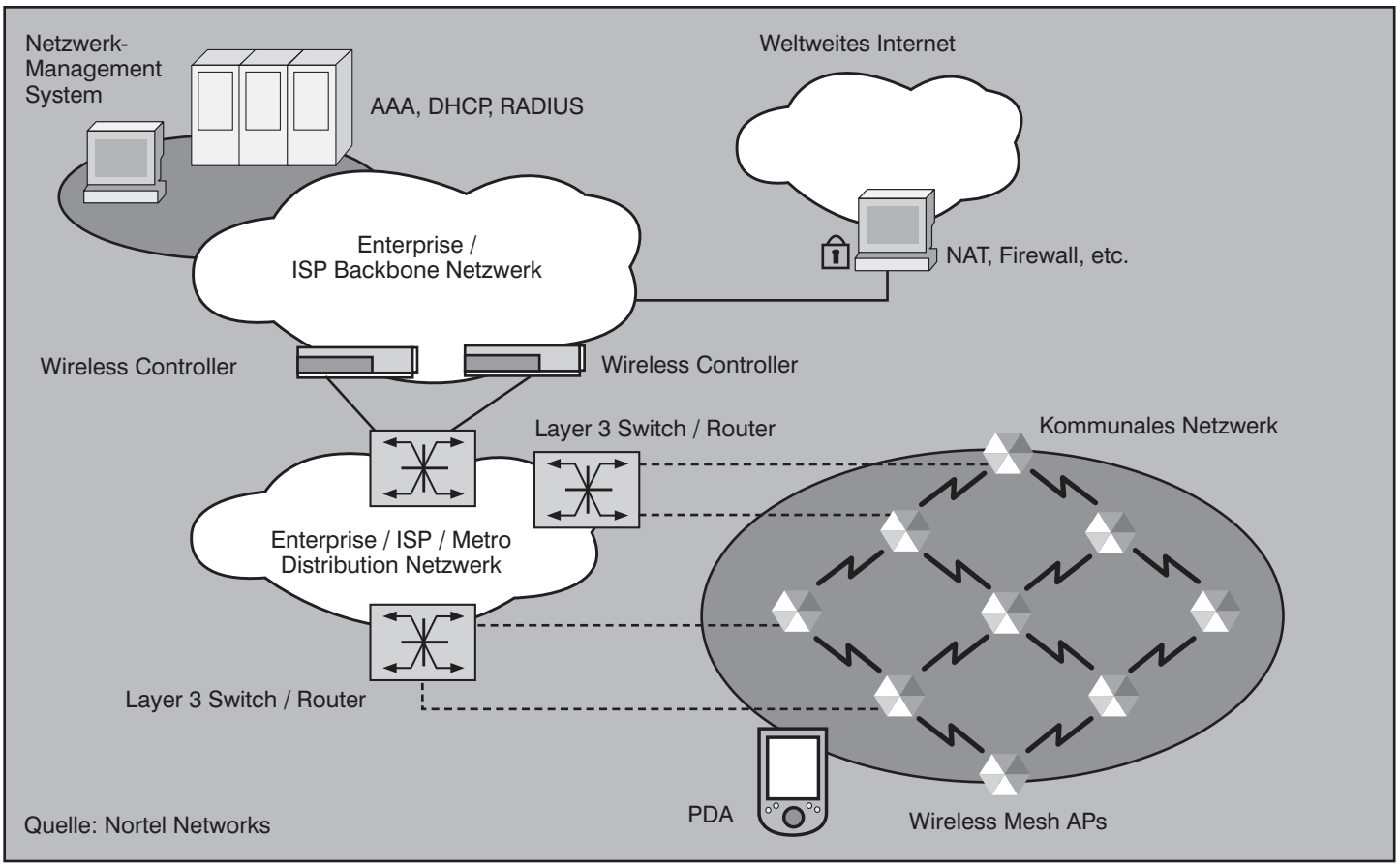


Abbildung 1.4: Fixed Mesh WLAN mit Übergang zum IP/Ethernet Netzwerk

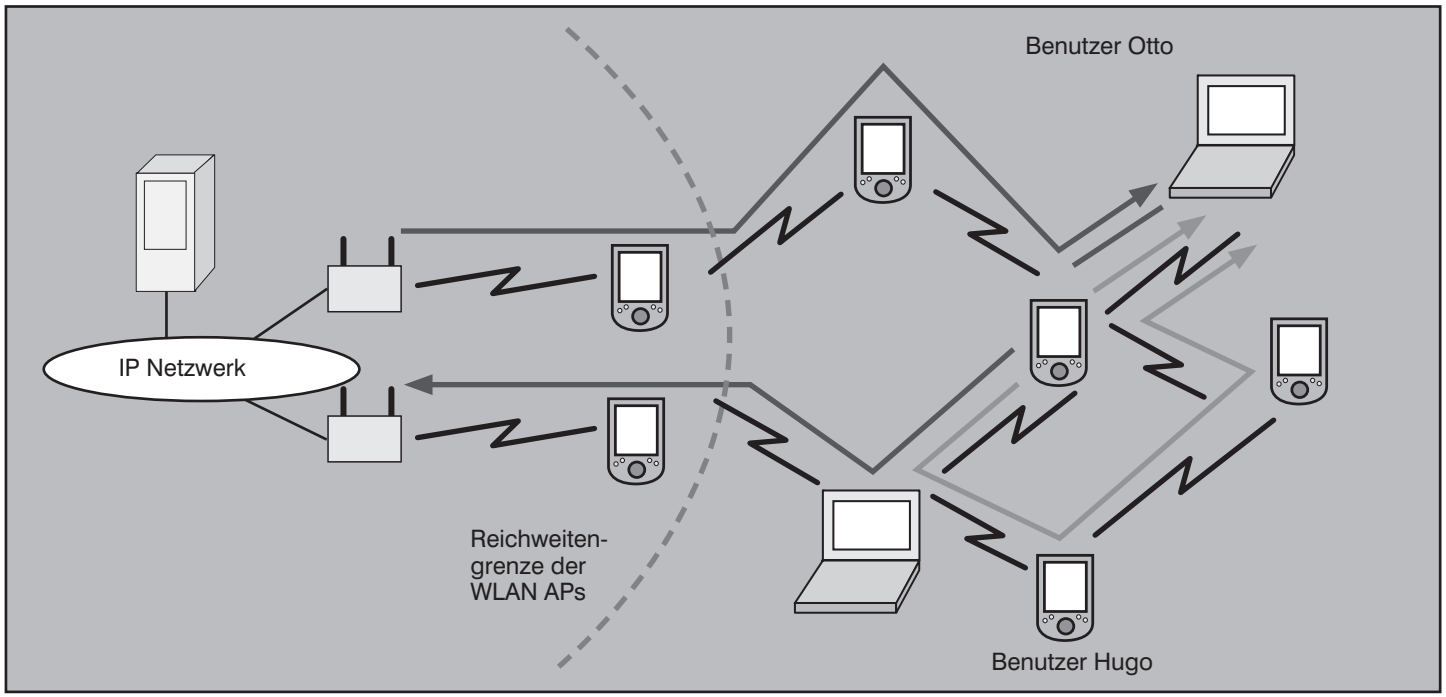


Abbildung 1.5: Client-Server Kommunikation unter Nutzung benachbarter Clients als Mesh Knoten

Eine weitere Typisierung berücksichtigt eher den Mobilitäts-Aspekt:

- **Fixed Mesh Networks:** Alle Routing Hops (Knoten) haben einen festen Standort (Infrastruktur-Komponenten)
- **Mobile Mesh Networks und MANETs (Mobile Ad Hoc Networks):** Alle oder mehrere Routing Hops (Knoten) sind beweglich (insbesondere auch Clients)

Die IEEE greift bei der Standardisierung von Mesh WLAN's nicht auf solche Typisierungen zurück sondern beschränkt sich auf die Definition der Funktionalität der verschiedenen Mesh Komponenten, ohne vorzuschreiben, ob diese in einem Client oder in einer Infrastruktur-Komponente implementiert ist. Somit steht der Standard allen Herstellern und Produkten offen.

1.3 Vorteile von Mesh WLAN's und Einsatzbeispiele verfügbarer Produkte

Mesh WLAN's können aus mehreren Gründen vorteilhaft eingesetzt werden: Der Aufwand für Verkabelungs-Infrastruktur wird minimiert oder ganz vermieden. Dadurch werden die Infrastrukturkosten minimiert und eignen sich Mesh WLAN's für ad hoc Szenarien, in denen keine Verkabelung verlegt werden kann. Die Implementierung lässt sich einfach und schnell ausführen. Aufgrund von Selbstlern-Mechanismen wird der Betrieb vereinfacht und automatische Skalierbarkeit erzeugt. Die gute Skalierbarkeit entsteht durch das Prinzip „mehr Leistung einfach durch Montage von mehr Mesh Knoten" – sofern die Stromversorgung gelöst ist. Die Fehlerumschaltung erfolgt automatisch durch Nutzung alternativer Wege, solange diese vorhanden sind. Innerhalb der Funkstruktur funktioniert das Handover für Clients relativ schnell.

Bei den aktuellen Lösungen setzen sich Fixed Mesh WLAN's gegenüber MANETs durch, da sie folgende Vorteile bieten: Fest positionierte Mesh Komponenten bieten Connectivity und Robustheit in einem Maß wie es bei mobilen Knoten nicht immer möglich ist. Eine Belastung des Endgeräts durch Forwarding und Austausch von Forwarding Informationen wird vermieden, die Endgeräte sind leistungsmäßig entlastet und kein Bottleneck mehr. Die konsistente Abdeckung flächiger Be-

reiche erfolgt durch stationäre Mesh Points / Mesh Access Points, es können keine Versorgungslücken aufgrund von divergenter Bewegung mobiler Mesh Points entstehen.

Typische Einsatzbereiche vermaschter WLAN's sind

- Öffentlicher Zugang in Metro-Bereichen
- Mobile Mitarbeiter von Stadtverwaltungen (Sozialarbeit, Ordnungsamt, ...)
- Öffentliche Sicherheit, Videoüberwachung (Polizei, Feuerwehr)
- Medizinischer Notdienst
- Katastrophen-Absicherung / Überbrückung, Mess-Stationen, Sensoren
- Gesundheitszentren, Krankenhäuser
- Produktionsbereiche, Warenannahme, Logistik
- Unternehmens-Gelände, Industrieparks
- Warenhäuser, Einkaufszentren
- Bahnhöfe, Flughäfen, Häfen
- Veranstaltungszentren, Theater, Kongresszentren
- Stadien, Erlebnisparks
- Last Mile Netzwerk-Erweiterung von Service Providern

Nachfolgend stellen wir einige Einsatzszenarien vor, die aktuell mit verfügbaren Produkten, zukünftig auch mit standardkonformen Produkten realisiert werden können.

Einsatzbeispiel 1:
Kommunales Netzwerk
Abbildung 1.4 zeigt ein kommunales Netzwerk, das als Fixed Mesh WLAN realisiert ist und für den Serverzugang über vier Portale an einen Metro Ethernet Backbone mit Controllern, Managementsystem und Sicherheits-Infrastruktur angebunden wird.

Einsatzbeispiel 2:
Mobile Mesh Netzwerk
Ein einfaches Client / Mobile Mesh Szenario zeigt Abbildung 1.5.: Hugo kann Daten mit Otto über zwei verschiedene Wege austauschen, wobei die Software auf Hugo's PDA hierfür die optimale Route berechnet und ausgewählt hat. Sowohl Hugo als auch Otto haben, obwohl sie sich aktuell beide außer Reichweite des nächsten Access Points bewegen, jeweils mehrere Routen durch das vermaschte WLAN hindurch zum Transit-Access Point, über den sie den Server erreichen.

Einsatzbeispiel 3:
Notfalldienste in San Francisco
In San Francisco hat das Kalifornische Amt für Notfalldienste ein Mobiles ad hoc Netzwerk implementiert, das insbesondere auch Videokamera-Überwachung unterstützt (IEEE 802.11b WLAN NIC's von Proxim oder 3e Technologies Internat. mit einer Reichweite von 500 m bis 830 m, Mesh WLAN Software von PacketHop). In einem Piloten waren bis zu 30 Personen gleichzeitig aktiv, die Video-Auflösung betrug ¼ VGA.

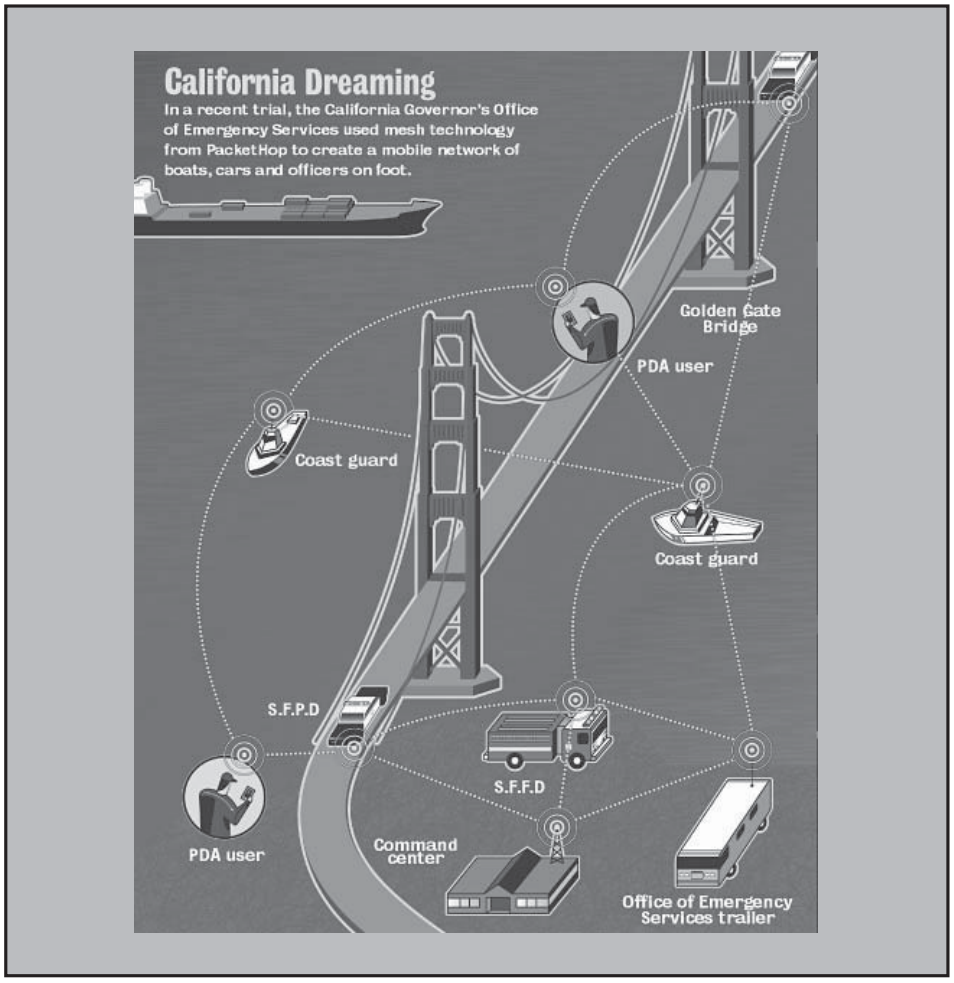


Abbildung 1.6: San Francisco WLAN Pilot für Notfall-Szenarien

In einem solchen vermaschten Mobile ad-hoc Netzwerk lassen sich zusätzlich zu den mobilen Mitarbeitern, die zu Fuß unterwegs sind, z.B. auch Boote der Küstenwache, Polizeifahrzeuge, Feuerwehr-Fahrzeuge und mobile Leitstellen einbinden, die mit Client-Systemen bestückt sind. Die Ankopplung an einen Ethernet Backbone / RZ für den Serverzugriff erfolgt über Antennenstationen auf der zentralen Leitstelle. Eine Übersicht des Piloten zeigt Abbildung 1.6.

Einsatzbeispiel 4: Fixed Mesh WLAN mit Ethernet Front End Access Points
Im Regelfall sind Endgeräte / Clientsysteme über WLAN assoziiert. Das Beispiel zeigt jedoch einen Sonderfall für Portale: Anstelle einer Wireless Assoziierung von Stationen könnten auch mehrere Ethernet Clients auf eine gemeinsame Wireless Anbindung konzentriert werden; dies entspricht auch Client-seitig einer Portal-Funktion. In diesem Fall sind so genannte Front End AP's verfügbar, die die Clientsysteme über mehrere geswitchte Ethernet-Schnittstellen anschalten („Front-End Ethernet", z.B. FireTide). Solche Mesh WLAN's ersetzen die Backbone Verkabelungs-Infrastruktur, benötigen jedoch keine WLAN-Schnittstellen und Treiber in den Client-Systemen. In diesem Fall ist der Front-End AP ein Ethernet-Miniswitch mit 4 bis 8 Ethernet-Schnittstellen 10/100Base-TX und ein bis mehreren Backbone-Funkverbindungen über IEEE 802.11a/b/h/g (oder auch WiMAX!). Die von den Clients erwartete oder verarbeitbare Eingangs-Last findet ihre Limitierung somit nicht in der Summe der Ethernet-Schnittstellen sondern in der Summe der Funkschnittstellen. Ein Einsatz-Szenario mit Backbone AP's, Transit AP's sowie Front End / Client AP's mit und ohne Ethernet Schnittstellen ist in Abbildung 1.7 dargestellt.

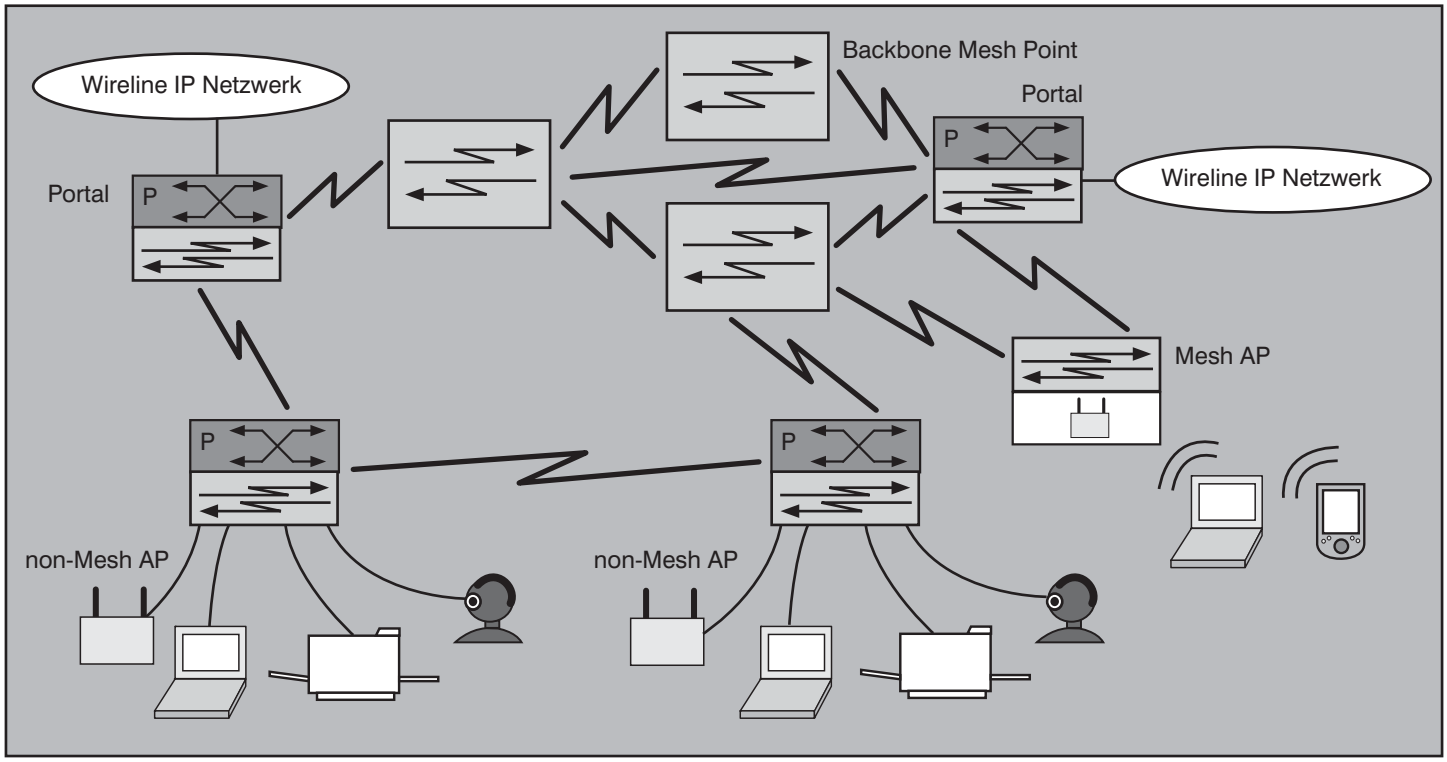


Abbildung 1.7: Mesh WLAN Einsatzszenario

1.4 Standardisierung von Mesh WLAN's: IEEE 802.1s

Aktuelle Lösungen für Mesh WLAN's nutzen zwar die Basis-Standards IEEE 802.11b/g/a/h (zukünftig auch 802.11n), erweitern den MAC-Dienst jedoch proprietär mit „Routing-Funktionalität" auf der Basis von Funk-Metriken, hin zu einer selbstkonfigurierenden Multihop-Topologie (Mesh) für Unicast und Multicast Transport. Hinzu kommen „proprietäre" IEEE 802.11i-Erweiterungen für den Betrieb von vermaschten Strukturen.

Die IEEE 802.11 Standardisierung arbeitet mit IEEE 802.11s an der Standardisierung einer vermaschten Lösung. Nachdem im Juli 2005 fünfzehn verschiedene Vorschläge eingereicht wurden (5 vollständige Vorschläge, 10 Vorschläge mit partieller Abdeckung), konnte die Arbeitsgruppe allerdings erst nach langer Diskussionszeit im September 2007 ein erster Konsens erreichen. Das inhaltlich abschließende WG Sponsor Ballot ist derzeit auf September 2008 terminiert, die finale formale Verabschiedung als eigenständiger Standard IEEE 802.11A auf August 2009 (siehe Abbildung 1.8). Der Standard wird Bezug nehmen auf QoS nach IEEE 802.11e / WMM und Sicherheit nach IEEE 802.11i / WPA. Die Nutzung und Einbindung aller MAC-Spezifikationen 802.11a/b/g/h/n versteht sich von selbst. Aufgrund der langen Zeitdauer ist gegebenenfalls von „pres" Vorimplementierungen, insbesondere des HWMP Protokolls, auszugehen. Daher geht dieser Beitrag an späterer Stelle detaillierter auf dieses Protokoll ein.

Ansatz der IEEE 802.11s WG
IEEE 802.11s definiert eine teils hierarchische, teils flache Struktur, in der prinzipiell nur MP (Mesh Points) die Vernetzung bilden. Sie leiten zwar Daten weiter, ermöglichen jedoch keine Assoziierung von Stationen. Hierfür sind MAP's (Mesh AP) erforderlich, die für die Stationen zusätzlich AP-Funktionalität haben.

2. IEEE 802.11s Mesh WLAN: Komponenten, Nutzungsmodelle, Architektur und Funktionen

2.1 Mesh WLAN Komponenten

Der Standard kennt folgende Komponenten in Mesh WLAN's (siehe)

- Station (STA)
- Mesh Access Poing (MAP)
- Mesh Point (MP)
- Mesh Point & Portal (MPP)

Station (STA): Wie in „normalen" WLAN's gibt es Stationen ohne Mesh Funktionalität, im Prinzip „normale" Clients, die sich wie gewöhnlich an einem Access Point assoziieren müssen, um kommunizieren zu können.

Mesh Access Point (MAP): Ein MAP ist eine Komponente mit **Mesh Funktion** zum Mesh Netzwerk und **AP**-Funktion zum Client. Er wird auch als Proxy für Clients bezeichnet, da er stellvertretend für sie die Weiterleitung der Daten übernimmt. Der MAP hat mindestens eine, im Regelfall mehrere Funkverbindungen zu andern MP/MAP/MPP. Um mit diesen zu kommunizieren und die Wege zu den adressierten Zielstationen zu finden, unterstützt er den „Mesh Dienst"

Im Prinzip ist ein MAP eine Kaskade von MP und AP.

Mesh Point (MP): Der Mesh Point arbeitet als reine **Relay Komponente** und sorgt für die effiziente und zuverlässige Verbindungs-Funktionalität innerhalb einer Masche (Mesh). Er hat hierfür mindestens zwei, im Regelfall mehrere Funkverbindungen zu andern MP/MAP/MPP und unterstützt den so genannten „Mesh Dienst", vielfach auch Mesh Routing genannt. Der MP kann keine Clients assoziieren (AP / Proxy Funktion fehlt) und hat keine Verbindung zu non-Mesh Netzen (Portal Funktion fehlt). Hier lässt der Standard jedoch eine Hintertür offen: als so genannte Collocation kann ein Mesh Point andere Komponenten (AP, Portal) integrieren.

Mesh Point & Portal (MPP): Das Portal stellt den **Übergang zu non-Mesh Netzen** dar, im Regelfall sind hier Ethernet/IP

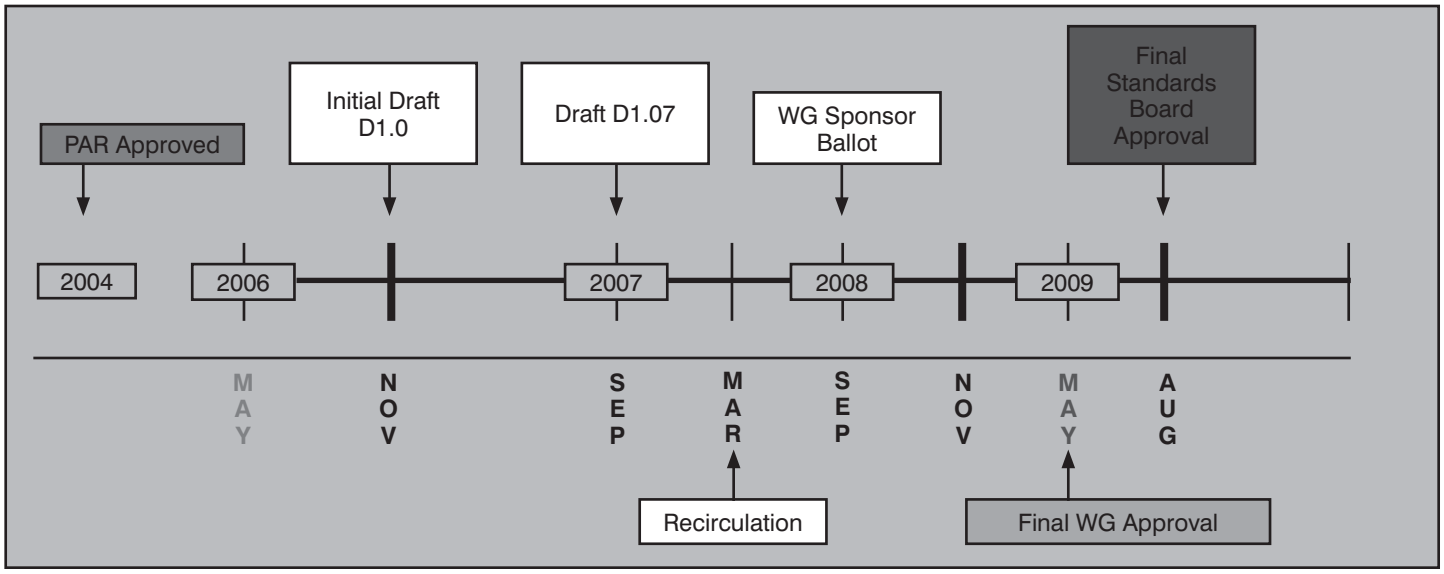


Abbildung 1.8: Zeitplanung des Standards IEEE 802.11s

(Backbones) zur Kommunikation mit Servern und Clients gemeint, die in einer verkabelten Infrastruktur angebunden sind; es könnten jedoch auch WiMAX Funknetze sein. Die Mesh Point & Portal Komponente hat mindestens eine, im Regelfall mehrere Funkverbindungen zu andern MP/MAP/MPP. Der MPP unterstützt den „Mesh Dienst", hat mindestens eine verkabelte Verbindung zu einem non-Wireless Netzwerk (Ethernet), unterstützt zum non-Wireless Netzwerk entweder IEEE 802.1D Brückenfunktionalität (optional mit Spanning Tree) oder aber Router-Funktionalität. Ein Mesh Point & Portal wird in Herstellerlösungen teilweise Mesh Router, Mesh Gateway oder auch Network Access Point (NAP) genannt.

Im Prinzip ist ein MPP eine Kaskade von MP und Brücke / Layer-2 Switch.

Wireless Bridge: Für Punkt-zu-Punkt-Verbindungen (P-t-P) über größere Entfernungen hinweg ist der Einsatz von Wireless Bridges möglich.

Eine Übersicht der Komponenten und Verbindungswege zeigt Abbildung 2.1.

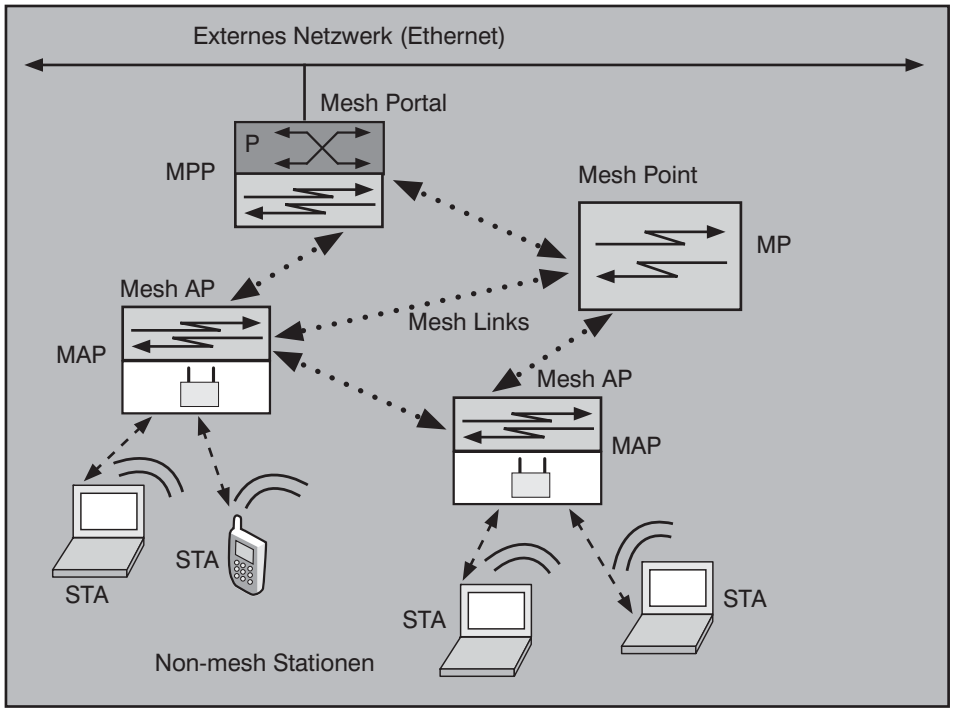


Abbildung 2.1: Komponenten eines Mesh WLAN

Eckwerte von IEEE 802.11s Mesh WLAN's

Die IEEE 802.11s Arbeitsgruppe hat mehrere, teilweise sehr unterschiedliche Nutzungsmodelle erarbeitet, für die der Standard einsetzbar sein soll. Typische Größen sind bis zu 32 Mesh AP's und max. 4 bis 5 Hops, bei Multiple Radio auch bis zu 10 Hops als maximaler „Mesh Durchmesser" (längster möglicher Weg). Für den Anschluss der Mesh Access Points ist ebenso wie für „normale" Acess Points eine Stromversorgung erforderlich! So werden z.B. Outdoor Access Points vielfach an Straßenlampen montiert und über deren Stromanschluss mit versorgt.

Wichtig: Die Anzahl der Übergänge zum Backbone / Internet / verkabelten Netzwerk begrenzt die Datentransfer-Summenleistung, da die Server im Regelfall im Backbone stehen.

2.2 Einsatz-Seznarios von IEEE 802.11 Mesh WLAN's

Szenario 1: SOHO Bereich

Für den SOHO Bereich sind Mesh WLAN's natürlich eine gute Alternative, da sie die Verlegung einer flächigen Verkabelung ersparen und sowohl Consumergeräte als auch Datenvernetzung/Internet-Zugang unterstützen. Für SOHO wird eine Fläche von 100 m² bis 400 m² vorgesehen. Die Mesh Komponenten sind selbstkonfigurierend, zum Einsatz kommen Indoor MP mit keiner oder niedriger Mobilität. Das gesamte Mesh WLAN hat maximal 6 Stationen, bis zu 8 MAP's und einen Durchmesser von 2 bis 3 Hops. Die Stationen können auch MAP-Funktion haben. Die Kommunikation findet typischerweise innerhalb des Mesh WLAN's statt.

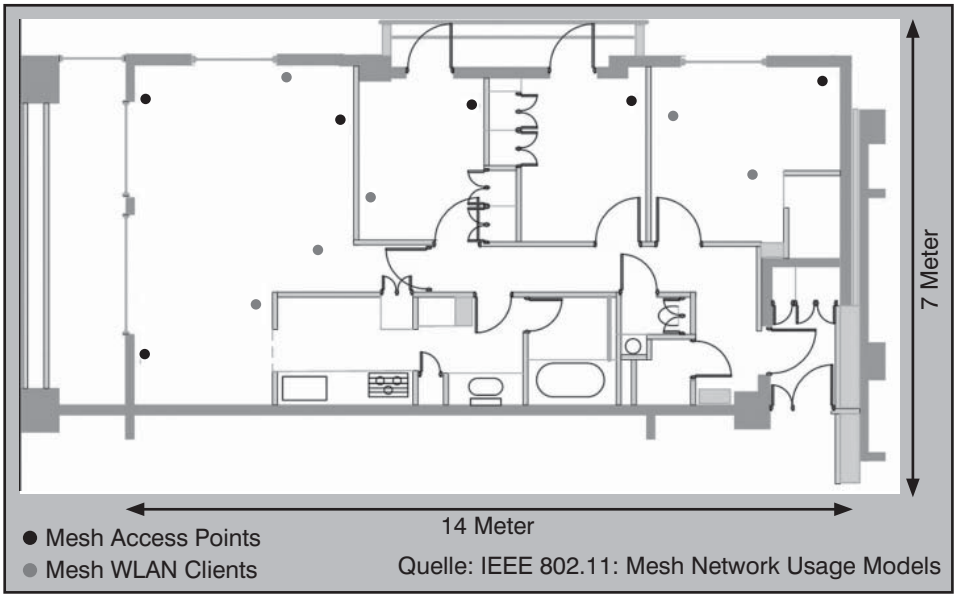


Abbildung 2.2: Nutzungsmodell SOHO Bereich

Eine Beispiel-Übersicht zeigt Abbildung 2.2, die schwarzen Punkte sind Mesh Access Points, die grauen Punkte sind mobile Stationen, d.h. Mesh WLAN Clients.

Szenario 2: Bürobereich
In Bürobereichen wird sich Mesh WLAN als Ethernet-Ersatz dort durchsetzen, wo schlechte räumliche Möglichkeiten für Verkabelungs-Infrastruktur gegeben sind oder als Ethernet-Ergänzung für Benutzer, die mobil unterwegs sind und mit niedrigerer Datenrate als am Arbeitsplatz auskommen. Auch bei Ad Hoc Netzen, die vorübergehender Natur sind (Messen, Medien-Events, etc.), kann die Montage / Demontage von Mesh Equipment deutlich kostengünstiger sein als die Installation / Deinstallation einer Verkabelungs-Infrastruktur plus flächiges Ethernet-Equipment. Für Bürobereiche wird eine Fläche von 1000 m² bis 8000 m² definiert. Die Mesh Komponenten sind selbstkonfigurierend, überwiegend ist der Einsatz von Indoor MP's ausreichend, gegebenenfalls erfolgt eine Erweiterung auf einige wenige Outdoor MP's. Alle MP/MAP's sind fest installiert. Im gesamten Mesh WLAN sind maximal 50 bis 300 Stationen zu versorgen, d.h. es ist von einer mittleren bis hohen Client-Dichte auszugehen. Bis zu 32 MP/MAP werden je Masche betrieben und bis zu 100 MP/MAP's in mehreren Maschen, die untereinander verbunden sind. Je Masche sind 5 bis 10 Portale vorhanden. Die Stationen haben nur in Einzelfällen MAP-Funktion. Die Kommunikation ist typischerweise Client-Server Kommunikation und nutzt somit bei jeder Kommunikations-Sequenz insbesondere die Portale. Eine Beispiel-Konfiguration zeigt Abbildung 2.3.

Szenario 3: Kommunales Netz
Für ein kommunales Netz wird eine Fläche von 1000 m² bis x000 m² definiert, die

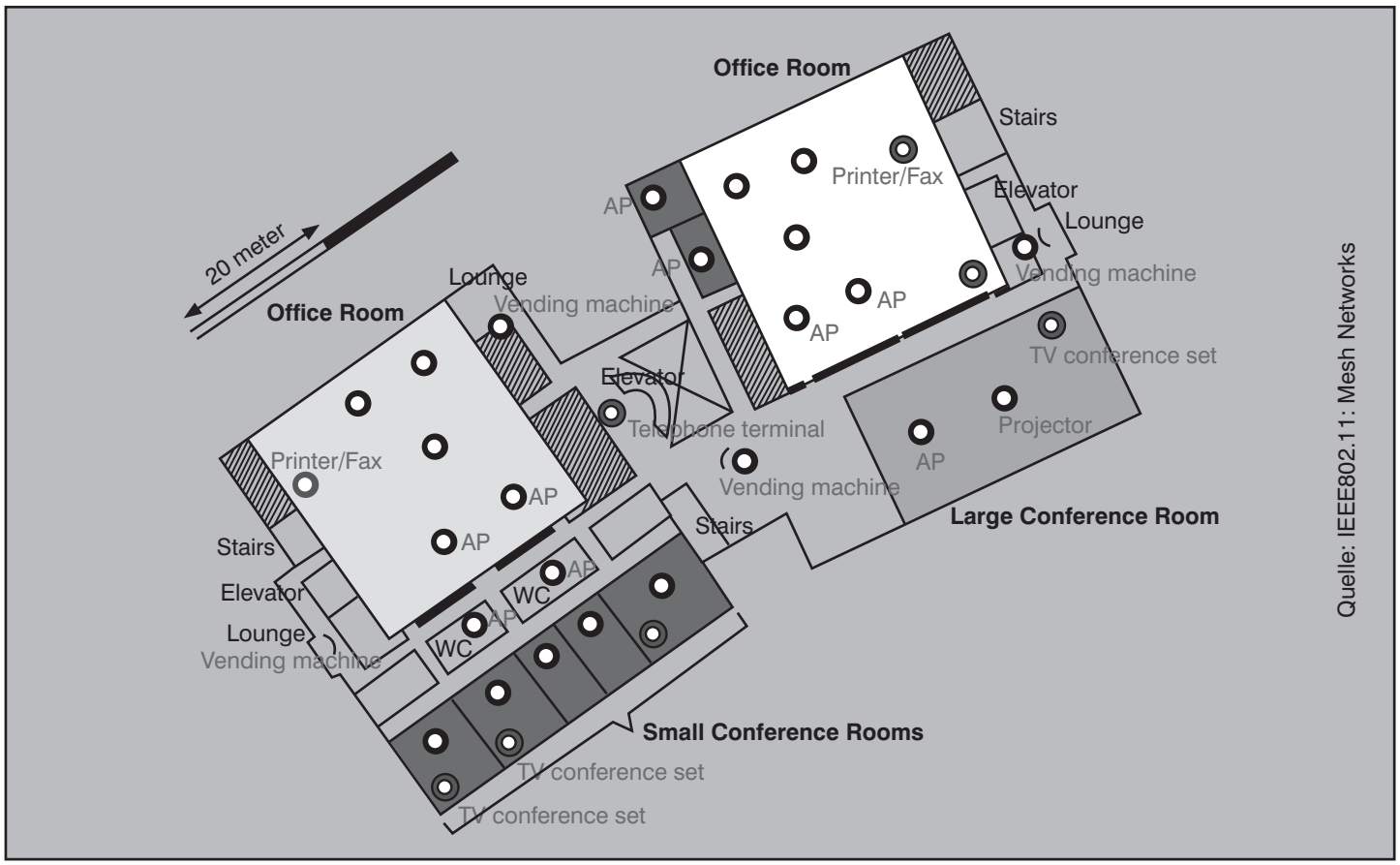


Abbildung 2.3: Nutzungsmodell Bürobereich

sich auf öffentliches Gelände erstreckt. Zum Einsatz kommen daher anders als im Bürobereich überwiegend Outdoor MP's, gegebenenfalls erfolgt eine Erweiterung auf einige Indoor MP' in öffentlichen Gebäuden. Alle MP's sind fest installiert, und die Mesh Komponenten sind selbstkonfigurierend. Die Stationszahl ist mit maximal 20 bis 1000 Stationen je nach Tageszeit und angebotenen / genutzten Diensten sehr variabel. Die Mesh Infrastruktur besteht aus bis zu 32 bis 100 MP/MAP je Masche und bis zu 50 oder 100 MP/MAP's in mehreren Maschen, die untereinander verbunden sind. Je Masche sind 5 bis 10 Portale vorhanden, hierzu gehören mindestens 2 Portale für hierarchische Maschenbildung. Die Stationen haben nur in Einzelfällen MAP-Funktion. Die Kommunikation ist typischerweise eine Client-Server Kommunikation nutzt insbesondere die Portale. Ein Beispiel-Szenario zeigt Abbildung 2.4.

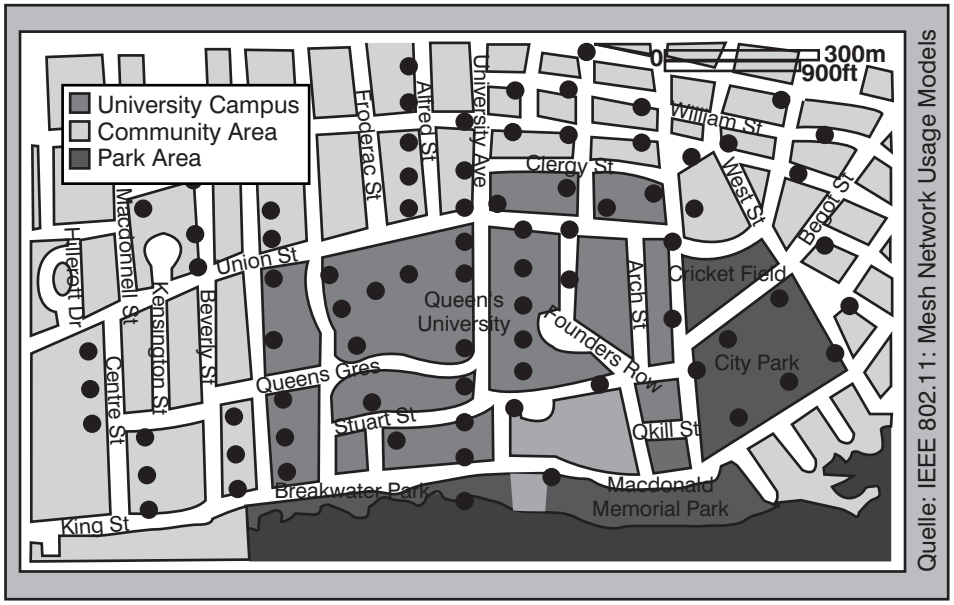


Abbildung 2.4: Nutzungsmodell Kommunales Netz

Szenario 4: Öffentliche Sicherheit, Notfall-Szenario

Für ein Notfall-Szenario (Brand, Hurrikan, Flutkatastrophe, Erdbeben, Terroranschlag …), das bei zerstörter Verkabelungs-Infrastruktur ad-hoc Netze für Polizei, Feuerwehr, Notärzte, Katastrophenschutz, THW etc. erfordert, wird je nach Ausdehnung der Katastrophe oder Notlage eine sehr variable Fläche von 250 m² bis x km² definiert. Die Mesh Komponenten sind selbstkonfigurierend, zum Einsatz kommen wie im kommunalen Netz überwiegend Outdoor MP's, gegebenenfalls erfolgt eine Erweiterung auf einige Indoor MP's, z.B. im Leitstand. Die MP's sind sowohl fest installiert als auch mobil. Die Stationszahl ist mit maximal 30 bis 250 Stationen je Masche kleiner als in kommunalen Netzen, da hier im Regelfall nur Sicherheitskräfte und technischen Hilfsdienste an der Kommunikation teilhaben; Stationen können MAP-Funktion implementiert habe, da insbesondere im Katastrophenfall natürlich ein hoher Beweglichkeitsfaktor für das gesamte Einsatzgebiet wichtig ist. Die Mesh Infrastruktur besteht aus bis zu 32 bis 100 MP/MAP je Masche und bis zu 50 oder 100 MP/MAP's in mehreren Maschen, die untereinander verbunden sind. Die Anzahl der Portale ist mit 5 bis 20 je Masche relativ hoch, was aus Redundanz- und Leistungsgründen in einem Katastrophenfall viel Sinn macht. Die Kommunikation verläuft sowohl intern als auch als Client-Server Kommunikation über die Portale hinweg. Ein Beispiel-Szenario zeigt Abbildung 2.5.

Szenario 5: Ad Hoc Szenario, Militäreinsatz

Für ein Militär-Szenario wird wie bei Szenario 4 eine sehr variable Fläche von 250 m² bis x km² definiert. Die Mesh Komponenten sind selbstkonfigurierend, zum Einsatz kommen überwiegend Outdoor MP's, gegebenenfalls erfolgt eine Erweiterung auf einige Indoor MP's. Die MP's sind sowohl fest installiert als auch mobil. Ein Ad Hoc Mesh WLAN soll maximal 30 bis 250 Stationen je Masche unterstützen; Stationen können auch MAP-Funktionalität besitzen. Die Mesh Infrastruktur besteht aus bis zu 32 bis 100 MP/MAP je Masche und bis zu 50 oder 100 MP/MAP's in mehreren Maschen, die untereinander verbunden sind. Die Anzahl der Portale ist mit 5 bis 20 je Masche wie beim Katastrophenfall relativ hoch. Die Kommunikation verläuft aber im Gegensatz zum Notfall-Szenario überwiegend intern, jedoch muss für einzelne Kommunikations-Sequenzen auch Client-Server Kommunikation über die Portale hinweg möglich sein (z.B. Gefechtsmeldungen an die Einsatzleitung). Ein Beispiel-Szenario zeigt Abbildung 2.6.

2.3 Architektur und Funktionen

Wie üblich sind ist auch der Mesh WLAN Standard in PHY, MAC und höhere Layer aufgeteilt. Im Physical Layer finden wir die typischen Schnittstellen IEEE 802.11a/b/g/h/j/n, da Mesh WLAN's mit allen ver-

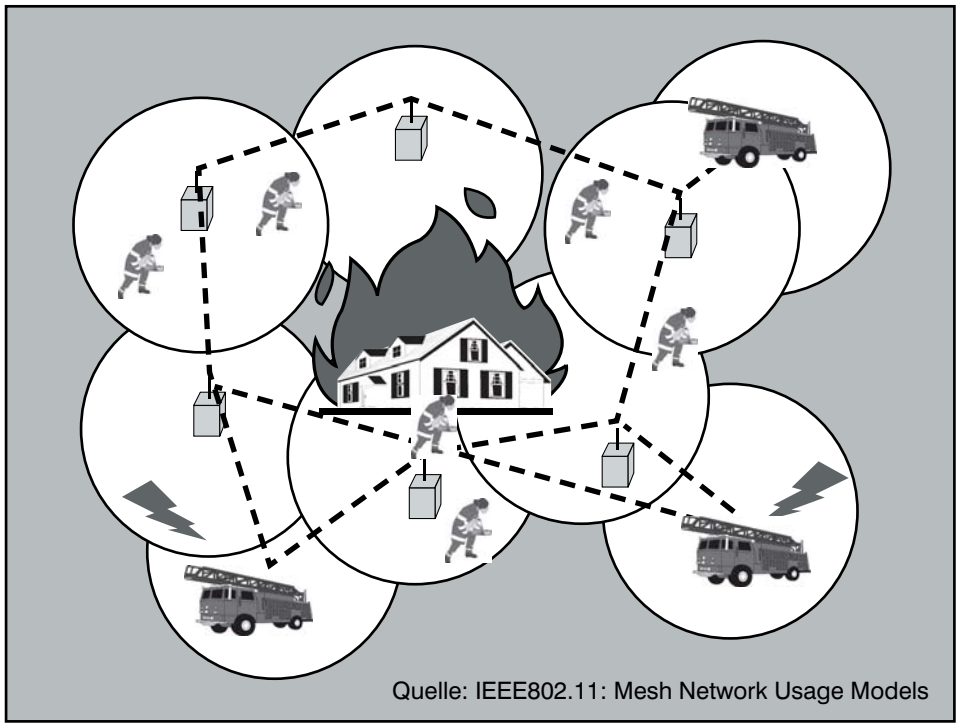


Abbildung 2.5: Nutzungsmodell für öffentliche Sicherheit

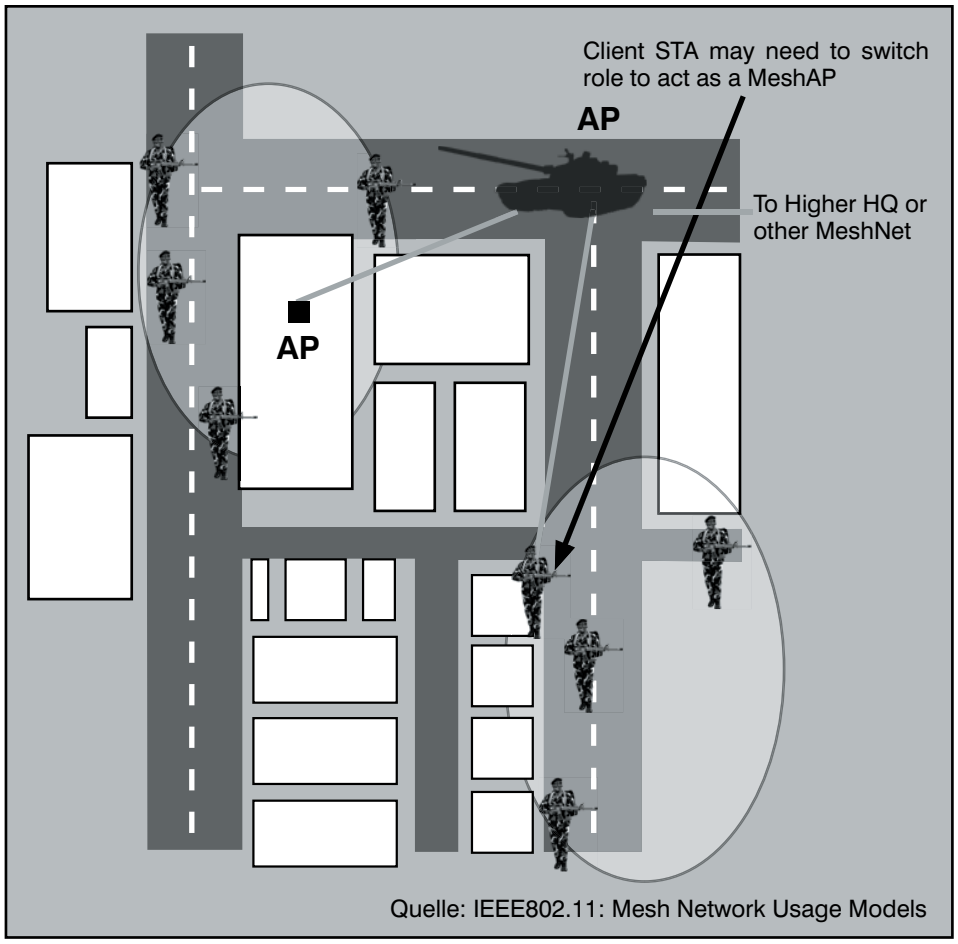


Abbildung 2.6: Nutzungsmodell für Ad Hoc Netze, Militäreinsatz

abschiedeten MAC Standards zusammen funktionieren sollen. Der MAC Layer ist in einen Sublayer für Mesh Erweiterungen (802.11e / n+) sowie mehrere Funktionsmodule zur Realisierung des Mesh Dienstes unterteilt. Als Schnittstelle zu den höheren Schichten wurden die Module Interworking sowie Mesh Konfiguration und Management definiert. Eine Übersicht zeigt Abbildung 2.7. Die einzelnen Funktionsmodule werden im folgenden näher beschrieben, sie wurden im Vergleich zum ursprünglichen Modell der WMA weiterentwickelt siehe Artikel im Insider März 2006.

Mesh Topology Learning, Routing und Forwarding: Dieser Block enthält Funktionen wie Nachbar Discovery, Radio Metriken, Routing Protokoll auf Basis von MAC Adressen und Weiterleitungs-Funktion. Das Routing Protokoll kann nicht OSPF sein sondern muss Metriken mit Radio- und Kanalparametern nutzen, um eine effiziente Wegwahl und Ressourcen-Nutzung zu ermöglichen

Netzwerk Messungen: Hier erfolgt zum einen die Berechnung der Radio Metriken zur Nutzung durch das Routing Protokoll, zum anderen werden Messungen von Funkbedingungen für eine optimierte Kanalauswahl durchgeführt

Mesh Medium Access Coordination: beinhaltet Funktionen für QoS zur Vermeidung von Leistungseinbrüchen, die bei Burst-Sendern oder für Clients an exponierten Stellen auftreten könnten. Hinzu kommen Funktionen für Prioritätskontrolle, Überlastkontrolle, Zugangskontrolle und effiziente Funkfrequenz-Nutzung

Mesh Security: deckt den Schutz für Daten- und Management-/Kontrollframes (insbesondere Routing Kontrollframes) ab und setzt die Nutzung von IEEE 802.11i Sicherheits-Schemas voraus

Mesh Interworking: bildet die Schnittstelle „nach oben“ zu anderen vermaschten WLAN‘s oder zu einem verkabelten Backbone. Hier wird die Portal-Funktion realisiert. WLAN Mesh Netze müssen konform zur IEEE 802 Netzwerk-Architektur arbeiten und entsprechend eine transparente Brückenfunktion zu anderen Netzen leisten.

Mesh Konfiguration und Management: definiert eine Schnittstelle, um die notwendigen WLAN Parameter für RF-Parameter (Sendeleistung, Frequenz-/Kanalwahl etc.), QoS Policy, Konfiguration etc. automatisch zu setzen

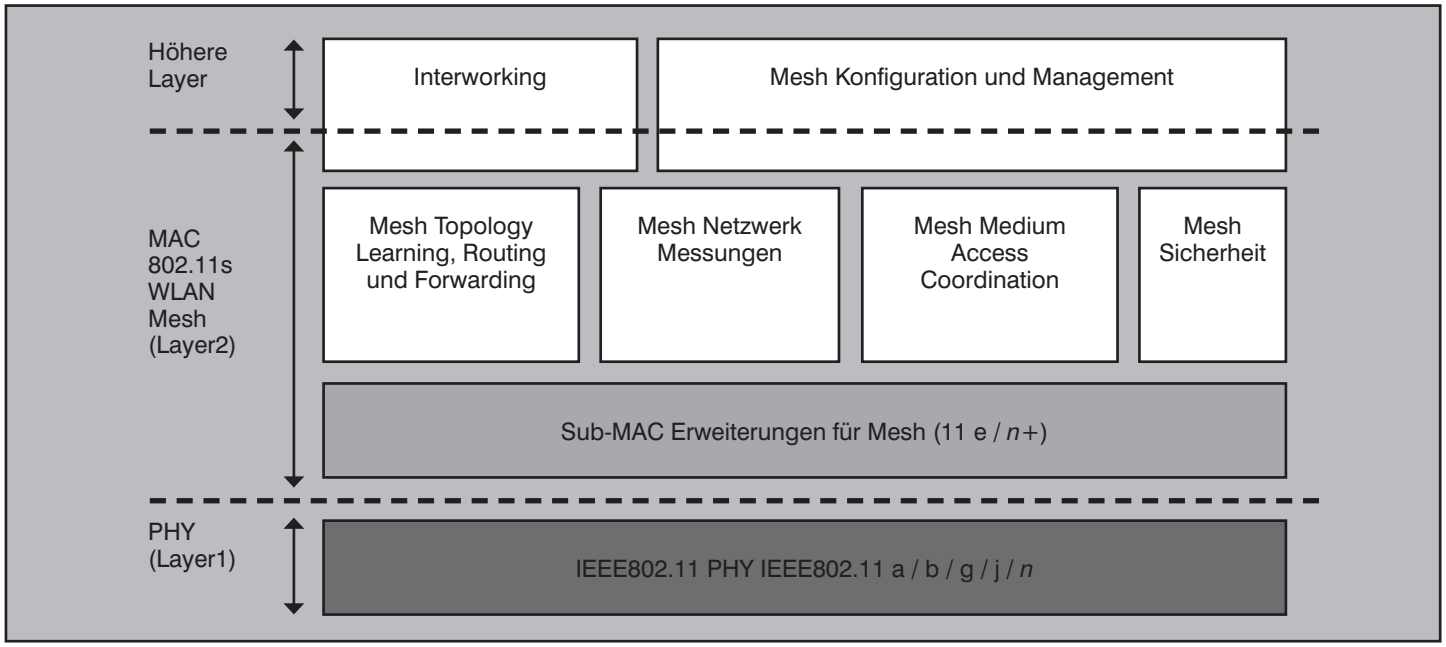


Abbildung 2.7: Funktionsmodule von IEEE 802.11s

Im Einzelnen werden damit alle notwendigen Funktionen eines Mesh WLAN abgedeckt:

- Funktechnik
  - Nutzung der lizenzfreien Frequenzbänder (IEEE 802.11)
  - Unterstützung von Indoor- und Outdoor-Bereichen
  - Unterstützung von Einfach-Antennen (Single Radio) und Mehrfach-Antennen (Multiple Radio)
- Maschenbildung
  - Funk-Eingangs-Schnittstelle (Mesh Ingress) und Funk-Ausgangs-Schnittstelle (Mesh Egress) an einem Knoten / Client
  - Portal: Optionale Ethernet Ausgangs-Schnittstelle(n) an einem Portal-Knoten, die eine Verbindung zu Ethernet-Geräten oder Backbone-Netzen herstellen
- Autodiscovery zwischen Mesh Points
- „Self-Healing“: Dynamisches Rerouting / Fehlerumschaltung
- Wegeoptimierung (Best Path)
- Load Balancing
- Automatische Erweiterbarkeit (Autokonfiguration)
- Sicherheit: Erweiterung von IEEE 802.11i auf vermaschte Topologien: Authentifizierung der Knoten; Nutzung von Verschlüsselung für Peer Links
- Optional: Autorisierung, Verschlüsselung
- Optional: QoS für Unicast und Multicast
- Standard-konformer Client Dienst (soweit Clients nicht Mesh Knoten sind): Assoziierung am Mesh Access Point
- Schnelles Client Handover zwischen Mesh Access Points
- Selten: Wireline Clients: Optionale Ethernet Front-End Eingangs-Schnittstellen am Mesh Access Point zur Anbindung von Endgeräten, die kein Wireless unterstützen

Abkürzungen Teil 1

AC	Access Controller
ACL	Access Control List(e)
AP	Access Point
ATP	Adaptive Transmission Protocol (MeshNetworks)
AWPP	Adaptive Wireless Path Protocol (Cisco)
BSS	Basic Service Set
CAN	Community Access Network (Nortel)
CAPWAP	Control and Provisioning of Wireless
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
DARPA	DoD Advanced Research Projects Agency
DCF	Distribution Coordination Function
DIFS	DCF Inter-Frame Spacing
DLS	Direct Link Setup
DoD	Department of Defense (USA)
DRCA	Distributed Reservation Channel Access
DS	Differentiated Services
DS	Distribution System
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced DCF
ESS	Extended Service Set
FEC	Forward Error Correction
GSM	Global System for Mobile Communication
HCCA	HCF Controled Channel Access
HCF	Hybrid Coordination Function
HDTV	High Definition TV
HWMP	Hybrid Wireless Mesh (Routing) Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Inter-Frame Spacing
IP	Internet Protocol
LAN	Local Area Network
LB	Load Balancing
MAC	Media Access Control
MAN	Metropolitan Area Network (Stadtnetz)
MANET	Mobile Ad Hoc Networks
MAP	Mesh Access Point
MCF	Mesh Coordination Function
MEA	MeshNetworks Enabled Architecture (MeshNetworks)
MIT	Massachusetts Institute of Technology
MP	Mesh Point
MPP	Mesh Point & Portal
MSR	MeshNetworks Scalable Routing

NAP	Network Access Point
NIC	Network Interface Card (Coupler)
OSPF	Open Shortest Path First
PAN	Personal Area Network
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PHY	Physical Layer
PIFS	PCF Inter-Frame Spacing
PoE	Power over Ethernet
P-t-P	Point to Point
PWRP	Predictive Wireless Routing Protocol (Tropos)
QDMA	Quadrature Division Multiple Access (MeshNetworks)
QoS	Quality of Service
RAN	Regional Area Network
RF	Radio Frequency
RFSM	Radio Frequency Spectrum Management
RSM	Robust Security Network
RST	Rapid Spanning Tree
RSTP	Rapid Spanning Tree Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RZ	Rechenzentrum
S.F.F.D.	San Francisco Fire Department
S.F.P.D.	San Francisco Police Department
SA	Scheduled Access
SDTV	Standard Definition TV
SIFS	Short Inter-Frame Spacing
SNA	Systems Network Architecture (IBM)
SOHO	Small Office Home Office
SRI	Stanford Research Institute (*1946, Stanford University)
SSID	Service Set Identifier
STA	Station
SVP	SpectraLink Voice Priority
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TG	Task Group
THW	Technisches Hilfswerk
TK	Telekommunikation
TSPEC	Transmission Specification
TV	Television
TX	Transmitter
TXOP	Transmission Opportunity
UPnP	Universal Plug and Play
VGA	Video Graphics Array
VLAN	Virtuelles LAN
VoFi	Voice over Wi-Fi
VoIP	Voice over IP
WG	
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WITnet	Wireless Intelligent Transport Network (Accton)
WLAN	Wireless LAN
WMA	Wi-Mesh Alliance
WMM	Wi-Fi Multimedia
WMN	Wireless Mesh Network (Nortel)
WPA	Wi-Fi Protected Access

Links

www.accton.com
www.belairnetworks.com
www.cisco.com
www.dlink.de
www.firetide.com
www.ieee.org/11
www.ieee.org/16
www.interdigital.com
www.motorola.com
www.motorola.com/mesh
www.nexthop.com
www.nortel.com
www.packethop.com
www.sohoware.com
www.strixsystems.com
www.thomson.net
www.tropos.com
www.wimaxforum.org
www.wi-mesh.org

Fortsetzung folgt!

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 25.02. - 27.02.08 in Stuttgart

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert..

Preis: € 1.690,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 25.02. - 26.02.08 in Stuttgart

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.

TCP/IP und SNMP, 25.02. - 29.02.08 in Stuttgart

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.

Trouble Shooting in vernetzten Infrastrukturen, 04.03. - 07.03.08 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 10.03. - 14.03.08 in Aachen

In diesem 5-tägigen Intensiv-Seminar steht das Führungsverhalten des Projektleiters eindeutig im Mittelpunkt. Professionelles Moderieren, Präsentieren, Verhandeln und Teamleiten ist eine Kunst, die trainierbar ist. Anhand begleitender Rollenspiele und Praxisübungen werden die führungsrelevanten Eigenschaften klar verbessert.

Preis: € 2.290,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 10.03. - 12.03.08 in Frankfurt a.M.

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Diesem Ziel dient das Seminar.

Preis: € 1.690,- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 10.03. - 14.03.08 in Aachen

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

Preis: € 2.290,- zzgl. MwSt.

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten, 10.03. - 14.03.08 in Frankfurt a.M.

Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Preis: € 2.290,- zzgl. MwSt.

Trouble Shooting für Netzwerk-Anwendungen, 01.04. - 04.04.08 in Aachen

Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Preis: € 2.190,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
11.02. - 15.02.08 in Aachen
09.06. - 13.06.08 in Aachen
15.09. - 19.09.08 in Aachen
24.11. - 28.11.08 in Aachen

TCP/IP und SNMP
25.02. - 29.02.08 in Stuttgart
26.05. - 30.05.08 in Aachen
20.10. - 24.10.08 in Berlin

Internetworking
10.03. - 14.03.08 in Aachen
02.06. - 06.06.08 in Aachen
13.10. - 17.10.08 in Aachen

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Trouble Shooter

Trouble Shooting 1
04.03. - 07.03.08 in Aachen
17.06. - 20.06.08 in Aachen
09.09. - 12.09.08 in Aachen

Trouble Shooting 2
01.04. - 04.04.08 in Aachen
24.06. - 27.06.08 in Aachen
14.10. - 17.10.08 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt. (Einzelpreise: je € 2.190.--)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
18.02. - 22.02.08 in Aachen
05.05. - 09.05.08 in Bonn
22.09. - 26.09.08 in Bonn

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
10.03. - 14.03.08 in Frankfurt
23.06. - 27.06.08 in Bonn
03.11. - 07.11.08 in Bonn

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
07.04. - 11.04.08 in Aachen
25.08. - 29.08.08 in Aachen
01.12. - 05.12.08 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Voice Engineer

Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie
25.02. - 27.02.08 in Stuttgart
05.05. - 07.05.08 in Bonn
15.09. - 17.09.08 in Frankfurt
17.11. - 19.11.08 in Frankfurt

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
25.02. - 26.02.08 in Stuttgart
05.05. - 06.05.08 in Bonn
03.11. - 04.11.08 in Bonn

Alternative 1: IP-Telefonie evaluieren, planen, betreiben
11.02. - 13.02.08 in Berlin
04.06. - 06.06.08 in Königswinter
01.09. - 03.09.08 in Stuttgart
27.10. - 29.10.08 in Bonn

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
10.03. - 12.03.08 in Frankfurt
02.06. - 04.06.08 in Stuttgart
13.10. - 15.10.08 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.02. - 19.02.08 in Hamburg
10.06. - 11.06.08 in Bonn
08.09. - 09.09.08 in Bonn
17.11. - 18.11.08 in Frankfurt

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd. - RD1 - Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415
German Hotline of ComConsult-Research:
02408-955300

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

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

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