ComConsult Research

Der Netzwerk Insider

Februar 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

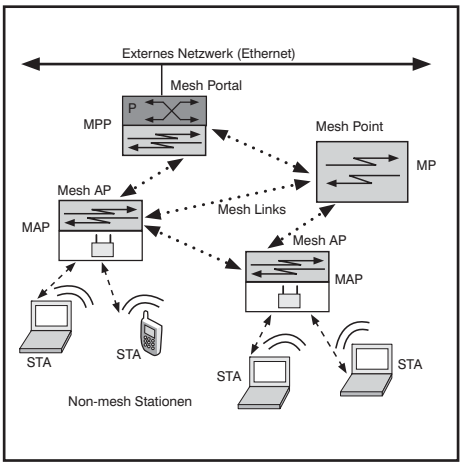
Schwerpunktthema

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 / Mesh-Networks, 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

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

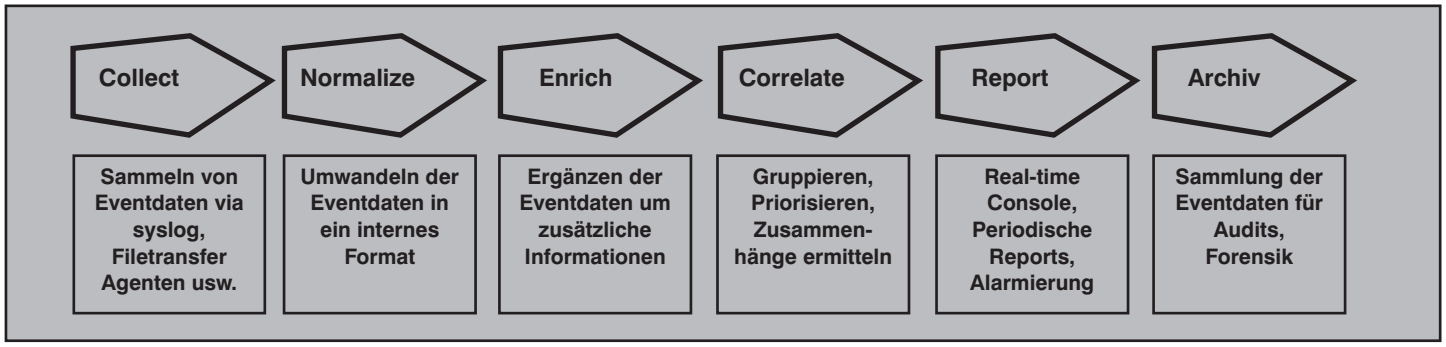


Abbildung 1: Der SIEM-Prozess

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

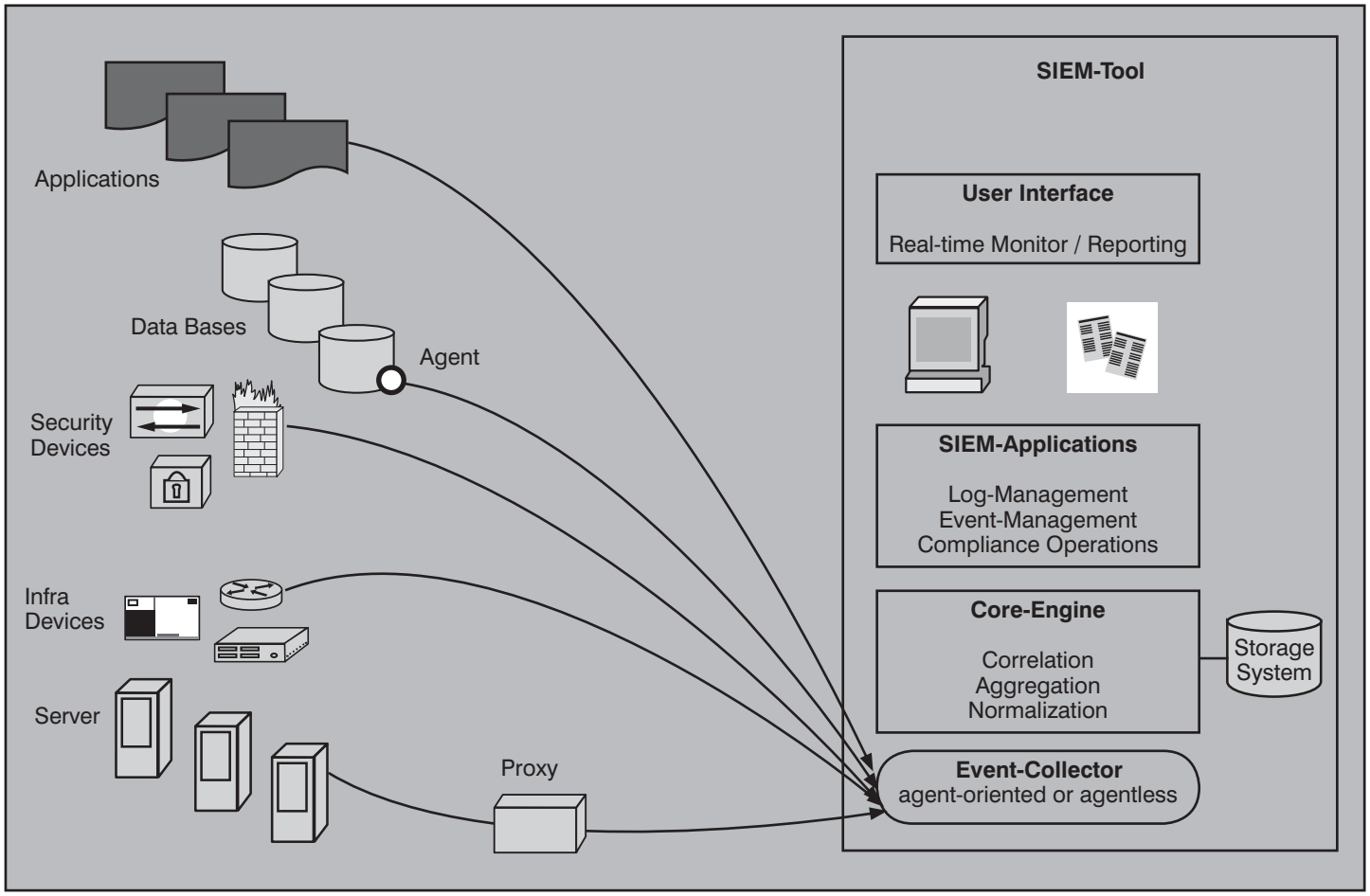


Abbildung 2: Komponenten einer SIEM-Lösung

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

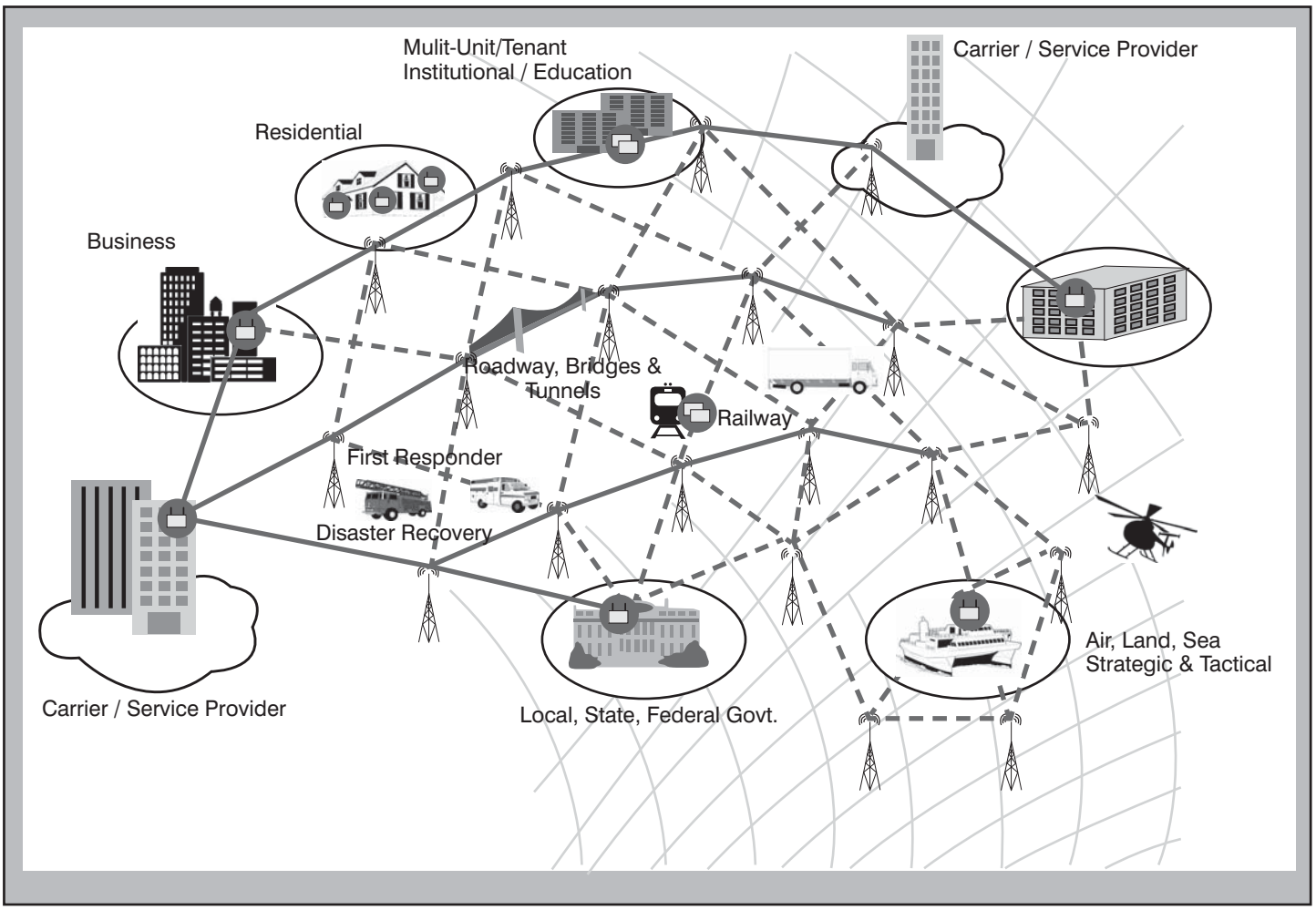


Abbildung 1.1: Vermaschte Wireless Netze

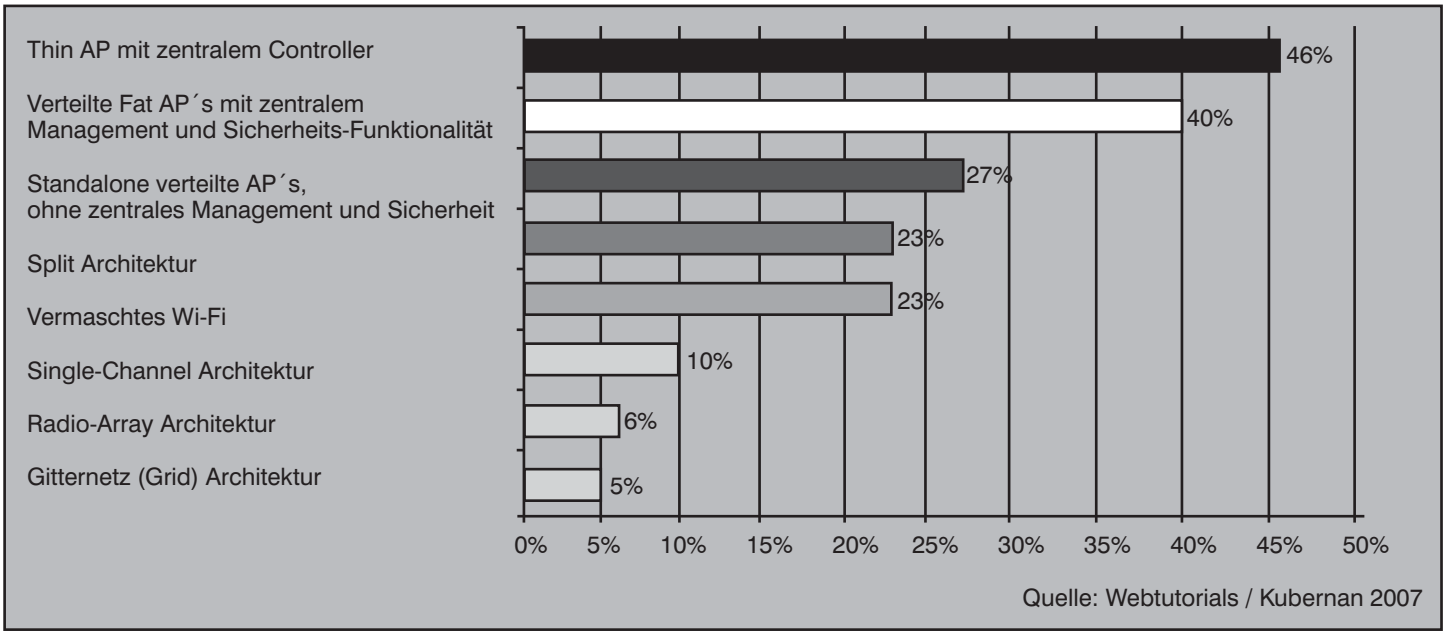


Abbildung 1.2: Verbreitung verschiedener WLAN-Architekturen

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).

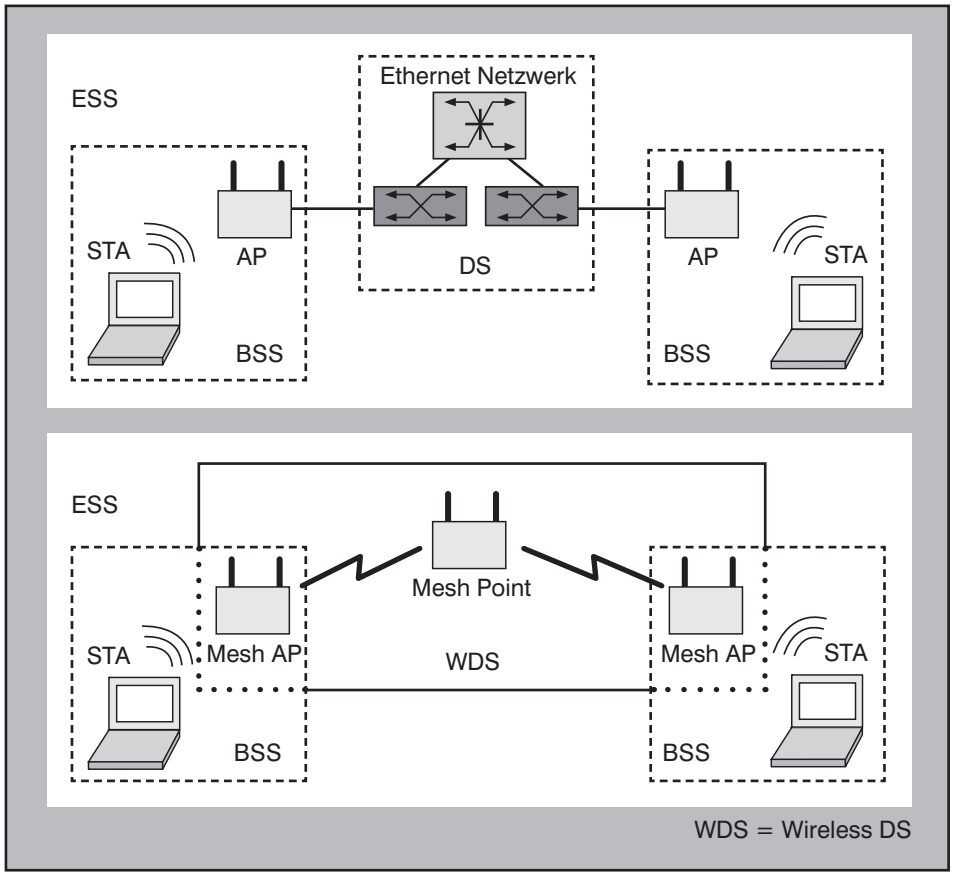


Abbildung 1.3: Vom Ethernet zum Wireless Distribution System

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.