ComConsult Research

Der Netzwerk Insider

Februar 2007

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Die Wireless Maschen-Netz Revolution und UWEs

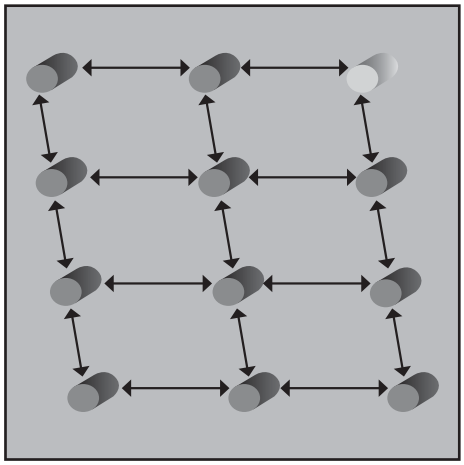
von Dr. Franz-Joachim Kauffels

Die bisherigen Standards/Drafts für Maschennetze IEEE 802.11s und IEEE 802.16a sind nur Wegbereiter für eine erhebliche Revolution auf dem Sektor der drahtlosen Netze. Die nächste Evolutionsstufe könnte weitgehend dezentralisiert und selbstorganisierend sein und hat damit ein erhebliches strukturelles Potenzial gegenüber herkömmlichen Konstruktionen. Eine wesentliche Komponente hierbei ist UWE, die Universal Wireless Entity.

1. Einführung

1.1 Notwendigkeit einer neuen Evolutionsstufe

Die Notwendigkeit für eine neue Evolutionsstufe ergibt sich immer dann, wenn die bisherige in eine konzeptionelle Sackgasse fährt. Dies ist heute bei den Wireless LANs eindeutig der Fall. Mit IEEE 802.11n steht zwar ein Standard für leistungsfähige WLAN-Zellen zur Verfügung, es gibt aber nach wie vor eine Reihe von Problemen, die auch mit 11n keineswegs einer angemessenen Lösung entgegenstreben. Aus meiner persönlichen Perspektive ist das Strukturproblem das bei weitem schwerwiegendste von allen. Was ist in den letzten Jahren passiert? Zunächst gab es einfach strukturierte WLANs mit der Aufteilung in Stationen, die die angebotenen Services eines Access Punktes nutzen und Access Points, die die grundsätzliche Struktur für eine Funkzelle schaffen und gleichzeitig „nach oben“ mit einem Distribution System an ein ganz normales LAN angeschlossen sind.



weiter auf Seite 20

Zum Geleit

Network Access Control NAC - Die Grundzüge einer neuen Technologie

von Markus Nispel

Mit NAC Network Access Control steht wieder einmal eine Technologie am Anfang des “Gartner Hype Cycles“ (http://www.gartner.com/pages/story.php.id.8795.s.8.jsp). Sowohl aus Sicht der Hersteller als auch aus Sicht der Kunden bietet NAC eine Reihe von Vorteilen und Möglichkeiten. Sie stellt aber auch eine Herausforderung insbesondere an die Struktur und Organisation desjenigen Unternehmens, das eine entsprechende NAC Lösung einsetzen möchte. In 2 bis 5 Jahren ist mit einer Mainstream Implementierung zu rechnen, wobei aktuell sich schon viele Unternehmen mit der Technologie auseinandersetzen und Teile davon implementieren bzw. schon implementiert haben.

Aktuell tummeln sich über 35 Hersteller in diesem Markt und die Zahl wächst fast täglich. Darunter sind auch einige der etablierten Player aus dem Netzwerk- und auch aus dem Security-Markt. Lt. Network Computing US Umfrage im Juni 2006 mit mehr als 300 Teilnehmern vertrauen 37% darauf, dass ein Netzwerkhersteller eine entsprechende Lösung bietet und 25% setzen auf einen bzw. ihren etablierten Securityhersteller. Man kann davon ausgehen, dass eine NAC Lösung aus Komponenten beider Lager bestehen wird.

weiter auf Seite 10

Top Veranstaltung

Netzwerk-Redesign Forum 2007

auf Seite 5

Geleit

Network Access Control NAC: zwischen Hype und Herstellerabhängigkeit

auf Seite 2

Report des Monats

Quality of Service in modernen Infrastrukturen

auf Seite 18

Zum Geleit

Network Access Control NAC: zwischen Hype und Herstellerabhängigkeit

Glaubt man den Prognosen, dann wird sich Network Access Control in den nächsten 3 Jahren zum absoluten Megathema entwickeln. Getrieben von einem realen Schutzbedürfnis einerseits und immer schärferen Auflagen andererseits bereiten sich immer mehr Unternehmen auf den Einstieg in diese Technologie vor.

Der Grundgedanke von NAC ist, dass nur Geräte und/oder Benutzer, die bestimmte Kriterien erfüllen, den Zugang zum Netzwerk und genau definierten Diensten im Netzwerk erhalten. Der noch relativ einfache Einstieg erfolgt über den Bedarf, einen geregelten Netzwerk-Zugang für Gäste einzurichten (und diesen dabei zum Beispiel den Zugriff auf das Internet oder auf Applikationen und Daten im Heimat-Netzwerk zu gestatten) oder mobile Mitarbeiter mit mobilen Endgeräten einer besonderen Sicherheitsprüfung zu unterwerfen.

NAC wird als Bearbeitungsprozess in der Regel in drei Phasen unterteilt, die nacheinander ablaufen:

1) Bewertung (assessment): ein Gerät und/oder ein Teilnehmer werden nach einem Prüfverfahren bewertet, zum Beispiel wird der Releasestand definierter Softwarepakete oder Treiber geprüft, die Aktualität des Virenschutzes wird sichergestellt und die Existenz einer lokalen Firewall abgefragt

2) Auswertung (validation): das Ergebnis der Bewertung, die typischerweise lokal durch einen Agenten erfolgt, wird an einen zentralen Policy-Server übermittelt, der nun nach vorgegebenen Regeln entscheidet, welche Zugriffsrechte dem Gerät/Benutzer erteilt werden

3) Umsetzung (Enforcement): durch Zuweisung der Endgeräte zu einem VLAN, was durch Parametrisierung des Switchports des für dieses Gerät zuständigen Access-Switches erfolgt, werden die Möglichkeiten, die das Gerät/der Benutzer im Netzwerk haben, festgelegt

Ein wesentlicher Ergänzungsprozess ist die Behandlung von Ausnahmen (exception handling). Dies betrifft einerseits Geräte, die keinen Agenten ausführen können und die deshalb eine Geräte-individuelle Behandlung zum Beispiel basierend auf der MAC-Adresse erhalten, aber auch andererseits Geräte, die durch Nichterfüllen von Kriterien in eine niedrige Zugangsklasse eingestuft werden und auf einmal keinen Zugang mehr zu wichtigen Unternehmensapplikationen erhalten. Im letzteren Fall kann es sinnvoll und wichtig sein, dass die zuständigen Gerätebetreiber und der User Help Desk informiert werden, um proaktiv vor dem Benutzer reagieren zu können.

So weit die heile Welt der Theorie. In der Praxis ist Network Access Control NAC mit einer Reihe von Problemen verbunden:

1) Es überschneiden sich Technologien und Zuständigkeiten zwischen Endgerät, Netzwerk und Applikation

2) Sinnvollerweise sollte der Agent Teil des Betriebssystems sein

3) Bei Netzwerken mit Netzwerk-Komponenten verschiedener Hersteller wird die Umsetzung schwierig

4) NAC setzt in der Regel einen bestimmten und vor allem einheitlichen Releasestand der Netzwerk-Komponenten voraus

Genau angesichts dieser Probleme können die bisherigen Lösungen nicht wirklich überzeugen. Sie sind sicher geeignet, um Teilfunktionen von NAC wie den Gastzugang abzudecken, aber für eine flächendeckende Umsetzung für alle vorhandenen Geräte sind die bisherigen Lösungen nicht geeignet.

Genau an dieser Stelle setzen jetzt die verschiedenen Initiativen an, die in dem Hauptartikel in dieser Insider-Ausgabe beschrieben werden. Im Kern versuchen diese Initiativen, ein Framework zu schaffen, um Technologie-, Hersteller- und Geräteübergreifende Lösungen umsetzen zu können. Zurzeit ist nicht sichtbar, dass sich die betroffenen Parteien auf einen Standard einigen (es gibt eine Arbeitsgruppe der IETF). Von der technischen Ausgangslage her wird kaum eine Lösung an dem Microsoft-Ansatz vorbei kommen. Die Einbeziehung des Betriebssystems und die Schaffung einer einheitlichen Schnittstelle zwischen Gerät und Policy-Server ist ein elementar wichtiger Schritt, der auch die organisatorischen Hürden zwischen PC- und Netzwerk-Betreibern überwinden kann. Es ist dabei nicht zu verstehen und eigentlich eine Zumutung, dass Microsoft dies nur für XP und Vista anbieten wird.

Bei den anderen Lösungen von Cisco und der TCG steht viel zu viel Politik im Vordergrund. Hier geht es den Herstellern nicht wirklich um eine tragfähige Lösung für den Kunden, hier geht es um pure Dominanz. Der Kunde soll in eine immer weiter gehende Abhängigkeit vom Hersteller getrieben werden. Wie schon seit Jahren üblich, wird dazu die Konfiguration und das Management von Komponenten als Vehikel missbraucht. Alle Kunden, die diesen Verlockungen in den letzten 10 Jahren gefolgt sind, können ein Leidenslied davon singen, wie häufig diese Konfigurationstools massiv geändert oder sogar abgekündigt worden sind.

Ich habe auch ernsthafte Zweifel an der Glaubwürdigkeit der Hersteller von Netzwerk-Komponenten (ich meine damit keinen bestimmten). Wer Netzwerk-Sicherheit ernst nimmt, der stellt als erste Stufe eine sichere zentrale Konfigurations-Verwaltung für seine eigenen Produkte zur

Verfügung. Diese sollte eine automatische Versorgung der Komponenten mit Firmware und Konfigurations-Parametern abdecken. Am liebsten natürlich auf einer genormten Plattform (SNMPv3???). Es ist unglaublich, dass Hersteller von NAC reden, aber gleichzeitig Konfigurationsparameter per TFTP oder FTP in Netzwerk-Komponent und IP-Telefone laden. Hier wird deutlich, dass es nicht um Sicherheit geht sondern im Macht und Dominanz.

Der Kunde ist hier in der Klemme. Noch ist keine der angebotenen Lösungen in einem Zustand, dass man sie großflächig ausrollen könnte. Dazu ist ein funktionsfähiges Framework erforderlich, das im Moment zeitlich gesehen von Microsoft abhängt. Diese Zeit sollten wir nutzen, um nach Alternativen Ausschau zu halten. Auf keinen Fall sollte man übereilt in NAC einsteigen. Die Gerätebetreuer und der Benutzerservice müssen Teil der Lösung sein. Dies erfordert klar und präzise definierte Ablaufprozesse. Sicherheit ist eine Organisations-Lösung, Technik ist hier nur ein Vehikel, um organisatorische Abläufe zur Umsetzung von Sicherheit möglich zu machen. Von daher steht die formale Beschreibung der Prozesse sowieso am Anfang. Wer seine Prozesse nicht formal festgelegt hat, der kann auch keinen Policy-Server konfigurieren, wo sollen die Regeln denn her kommen? Und mit der Erarbeitung der Prozesse ergibt sich die Chance, an eigenen Lösungen zu arbeiten und nicht den Marketing-Wolken der Hersteller zu folgen.

Jede sinnvolle NAC-Lösung sollte dabei die folgenden Grundregeln erfüllen:

1) Einfachheit: nur Zugänge regeln, die wirklich Sicherheits-relevant sind, NAC neigt vom Grundansatz her zu komplexen Lösungen

2) Neutralität: Komponenten mehrerer Hersteller müssen einbindbar sein, Zwei-Hersteller-Strategien sind wieder vermehrt in Diskussion und eine solche Lösung muss möglich sein

3) Technologie- und Organisations-übergreifend: es müssen klare und einfach handhabbare Schnittstellen zwischen Technologie- und Organisations-Bereichen bestehen

4) Vollständigkeit: alle Sicherheits-relevanten Geräte müssen einbindbar sein, also auch Geräte, für die es keinen Agenten gibt

5) Ausnahme-Behandlung: NAC wird zu 5 bis 10% schief gehen. Es wird immer Geräte geben, denen der Zugang verwehrt wird, obwohl sie diesen jetzt benötigen. Dafür müssen Lösungen vorgedacht werden

6) Alarm-Behandlung: NAC und Sicherheits-Monitoring gehören untrennbar zusammen. Wird ein Angriff erkannt, sei es durch den NAC-Agenten oder ein anderes Sicherheits-System, muss dies Auswirkungen auf den Policy-Server haben, der dann per Enforcement sofort zu reagieren hat

7) Kontinuität: Wie häufig und wann erfolgt die NAC-Überprüfung? Ist alles vorbei, wenn das Gerät einmal „drin“ ist? Hier scheiden sich momentan die Geister und unterscheiden sich die angebotenen Lösungen technisch. Jeder Kunde sollte seinen Bedarf diesbezüglich genau hinterfragen

Natürlich widmen wir uns dem Thema auf unserem Netzwerk-Redesign-Forum 2007. Wir greifen das Thema in mehreren Vorträgen, darunter ein zentraler, auf und diskutieren das Für und Wider dieser aufkommenden Technologie.

NAC ist sicher wie Sie an meinen Ausführungen gesehen haben, ein sehr kontroverses Thema. Aber ohne Frage bietet genau die offene und engagierte Diskussion auch die Möglichkeit, den Herstellern hier Grenzen aufzuzeigen und Lösungen zu fordern, die im Interesse des Kunden und nicht des Herstellers sind.

Ihr
Dr. Jürgen Suppan

TOP-Veranstaltung

Quality of Service - QoS

Einsatzbereiche, typische Fehler, optimale Nutzung

Quality of Service sorgt in der Theorie dafür, dass Ihre wichtigen Daten in Netzwerken immer mit hoher Qualität ankommen. Es dient dazu, Daten in Netzwerken in Verkehrsklassen einzuteilen, die dann unterschiedlich behandelt werden. Die Motivation kann sehr unterschiedlich sein:

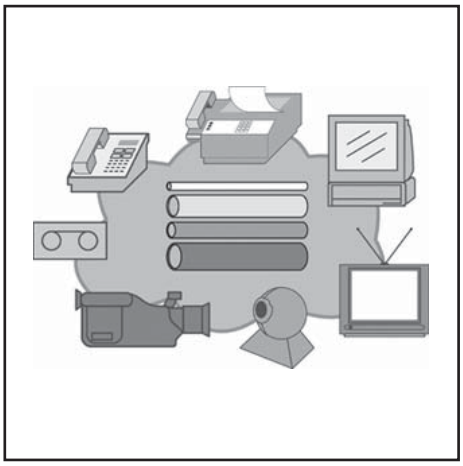
- Verhinderung der Behinderung wichtiger Daten durch unwichtige Daten
- Sicherstellung der Verfügbarkeit von Netzwerken für wichtige Anwendungen auch im Falle von Störungen
- Trennung von Applikationsdaten im Netzwerk

Die im Moment wogende Diskussion von QoS wird durch die Zunahme von Realzeitdiensten auf der einen Seite und der Notwendigkeit von Qualitätszusagen für die Dienste auf der anderen Seite erzeugt. Netzwerk-Betreiber werden zunehmend gezwungen, Maßnahmen zur Unterstützung wichtiger Dienste auch formal nachzuweisen.

QoS und Netzwerk-Sicherheit im Sinne der Trennung von Anwendungen und Benutzern im Netzwerk liegen naturgemäß nahe beieinander. In beiden Fällen werden Daten klassifiziert und unterschiedlich behandelt. Dies führt dazu, dass QoS und VLAN´s eng miteinander verzahnt sind.

Trotz der sehr einfachen Beschreibbarkeit der Ziele führt einen die Umsetzung von QoS in eine Reihe von Tücken und Problemen:

- QoS macht die Konfiguration von Netzwerken wesentlich aufwendiger und erschwert Betrieb und Monitoring
- QoS und VLAN-Konstrukte liegen nah beieinander und müssen in einem tragfähigen Konzept integriert werden. Dies



ist nicht trivial, bereitet doch gerade die Einbindung von Telefonen zunehmend Kopfschmerzen
- QoS für eine Applikation, für Teile einer Applikation oder für ein Gerät? Die Elementarfrage des QoS, so einfach gestellt so schwer umzusetzen
- Schlüsselfrage aller aktuellen QoS-Lösungen ist die Handhabung von Sprachanwendungen: wie soll ein IP-Telefon optimal angeschlossen werden, was ist mit einem Softphone, was passiert mit Sprachanwendungen auf dem PC (zum Beispiel Kollaborations-Anwendungen, Web-Conferencing usw), speziell dieser Anwendungsbereich steckt voller typischer Fehler, die unbedingt vermieden werden müssen
- QoS im Anschluss-/Etagenbereich definieren, aber am ersten Layer-3-Router zu terminieren ist sicher keine gute Idee. Bei vielen VLAN-basierten Konstrukten wird dies aber gemacht. Schon fast ein Konfigurations-Fehler. Dabei gibt es Technologien, um VLAN`s auch im Layer-3-Bereich zu trennen und QoS auch hier aufrecht zu erhalten
- QoS für Anwendungen mit hohen Bandbreiten? Hier droht die Blockade von anderen Anwendungen. Was bedeutet das für Voice und Video, wenn sie Erlang(k)=1 als traditionelle Gestaltung derartiger Netzwerke ansetzen?

Aus diesen Gründen ist die Einführung von QoS immer mit folgenden Rahmenbedingungen verbunden:

- Klares Konzept, einheitliche Handhabung, keine individuellen Lösungen
- Nur einsetzen, wenn nachweislich ein Zugewinn an Qualität und Stabilität erreicht wird
- QoS ohne ein betriebstechnisches Monitoring der angestrebten Qualitätswerte ist Unfug, zum einen muss geprüft werden, ob die Ziele erreicht werden zum anderen ermöglicht es Feintuning

Im Detail sind Quality-of-Service-Lösungen voller Tücken. Nicht selten erreichen sie ihre Ziele nicht, häufig werden Instabilitäten und Störungen geradezu produziert.

Unser hochaktuelles Seminar „Quality of Service“ setzt genau an dieser Stelle an. Lassen Sie sich vom international angesehenen Top-Netzwerk-Experten Dr. Behrooz Moayeri in die Feinheiten von QoS-Lösungen einführen. Lernen Sie, diese Technologien erfolgreich und sinnvoll zu nutzen. Im Interesse der Stabilität und Performance Ihres Netzwerkes, aber auch im Interesse eines geordneten Betriebs.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Quality of Service - QoS

☐ Ich buche das Seminar
Quality of Service - QoS
12.02. - 13.02.07 in Köln
zum Preis von € 1.390,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

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

Aktueller Kongress

Netzwerk-Redesign Forum 2007

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

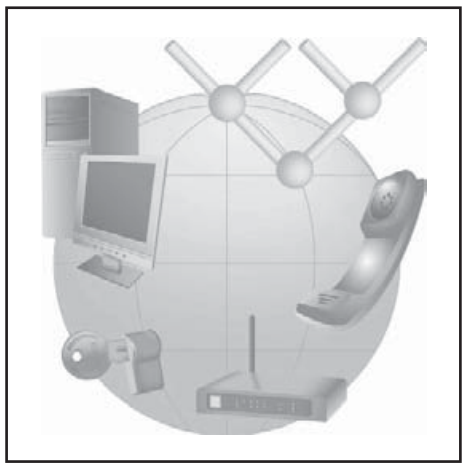
Alle Analysen, die wir exklusiv auf dem Netzwerk-Redesign-Forum vorstellen werden, sind aufgesetzt und in Arbeit. Als Vorgeschmack auf wichtige Diskussions-Themen des Forums greifen wir einige Aspekte im Folgenden heraus. Die Aufzählung ist noch nicht vollständig, wir werden Sie in den nächsten Wochen über weitere Themen informieren

Themenblock: Sicherheit und Beherrschbarkeit von Netzwerken
Folgende Aufgaben entstehen u.a. im Betrieb moderner Netzwerke:

- Sicherer Netzwerk-Zugang von IP-Telefonen bzw. Kommunikations-Applikationen
- Verhinderung des Netzwerk-Zugang für nicht autorisierte Personen und Geräte
- Trennung von Applikationen und Benutzergruppen im Netz, Verhinderung der Störung von Benutzergruppen und Anwendungen durch andere Benutzergruppen, Verhinderung von Sabotage bzw. Begrenzung der Auswirkung von Sabotage auf einzelne Anwendungen
- Sicherstellung von Verfügbarkeit und Qualität in unterschiedlichen Dimensionen für verschiedene Anwendungen

Diese Aufgaben sind nahe liegend, haben aber diverse Tücken, dazu einige Beispiele:

- Der Trend zum Unified Client im Bereich IP-Telefonie generell und speziell die Aktivitäten von Microsoft und Nortel (siehe Interview von Ballmer und aktualisierte Roadmap aus der letzten Woche) sorgen dafür, dass triviale VLAN-Konzepte zur Einbindung von Telefonen sich überlebt haben. Diese Konzepte sind mit der nun anstehenden Einbindung von Kommunikations-Funktionen auf dem PC überholt
- Generell stellt der gesamte Bereich der Anbindung von IP-Telefonen ein durchaus komplexes Thema dar, zu dem es keine perfekte Lösung gibt. Wir analysieren für Sie die Alternativen und berücksichtigen die neuesten Entwicklungen
- QoS- und VLAN-Konstrukte verzahnen sich unvermeidbar. Ein integriertes



Konzept ist gefordert, das auf der einen Seite Sicherheits-Fragen und auf der anderen Seite Performance- und Verfügbarkeits-Ziele integriert. Auch hier analysieren wir für Sie die Alternativen mit Vor- und Nachteilen

- Aufwendige VLAN-Konstrukte im Access-Bereich und im Layer-3 kommt alles zusammen. Ist das wirklich schlüssig? Wir geben Empfehlungen zu einer verbesserten Handhabung, die sich in den letzten Monaten im Markt etabliert hat
- Die Konfiguration von QoS/VLAN/Benutzertrennung/NAC ist komplex und fehleranfällig. Ein Monitoring der realen Betriebssituation und ein Soll-Ist-Vergleich ist deshalb im Tagesbetrieb unvermeidlich. Auch Feintuning und Optimierungen setzen Informationen über die reale Betriebssituation voraus. Die Grundregel: Sicherheit und Stabilität von Netzwerken ist ohne Monitoring nicht zu erreichen. Aber wie und wie umfangreich? Wir diskutieren diesen sehr schwierigen Themenbereich (Kosten, Betriebsaufwand, kein sichtbarer Nutzungen, wenn alles optimal ist)
- Das Hype-Thema in den USA ist zurzeit Network Access Control NAC. Die Hersteller puschen dieses Thema und generieren damit eine erhebliche Diskussion, die sich durch die amerikanischen Medien zieht. Das Thema ist technisch und organisatorisch komplex. Auf der technischen Seite stehen so schwierige Themen wie die Boot- und Zugangsreihenfolge unter Berücksichtigung von diversen Diensten sowie die Frage der Installation zusätzlicher Agenten auf den PCs. Auf der organisatorischen Seite steht die simple aber schwierige Frage der Zuständigkeit für den Netzwerk-Zugang und die Frage, wer die damit verbundenen Störungen bearbeitet. Wer betreut den Benutzer, dessen PC vom Zugang geblockt wurde und wie kann das in den Help-Desk eingebunden werden? Wir analysieren für Sie die bestehenden NAC-Varianten, erste Projekterfahrungen und die Frage, wie ein optimaler Mix aussehen kann.

Themenblock: Neue Technologien
Wir arbeiten noch an der endgültigen Liste, aber folgende Themen sind bereits klar:

NT1) WLAN-Technologien
Apple liefert seine neuen Endgeräte seit Herbst 2006 bereits mit 802.11n-Chips aus, die zugehörigen Access-Points kommen im Februar in den Markt. Intel hat gerade angekündigt, 11n ab Ende Januar als Teil des Centrino-Chipsatz auszuliefern. Die Integration in die Notebooks von Acer, Dell und Toshiba ist umgehend zu erwarten. Parallel hat Intel ein Interoperabilitäts-Zertifikat für 11n Access-Points geschaffen, das mögliche Probleme durch den Pre-Standard-Status beheben soll. Dieses Zertifikat steht in Konkurrenz zum Wifi-Zertifikat für 11n, das ab dem 2. Quartal angeboten werden wird. Die Arbeitsgruppe IEEE 802.11n hat diese Woche den Draft 2 freigegeben. Der Kern der Normung ist stabil, offene Diskussionen betreffen zum Beispiel spezielle Gerätegruppen wie Home-Entertainment. Die Chip-Hersteller sind jetzt in der Position, vorwärtskompatible Chips zu erstellen. Somit können alle Anbieter von 11n-Lösungen jetzt mit der Entwicklung der finalen Produkte beginnen. D-Link hat dementsprechend für Ende Q1 ein entsprechendes Produkt angekündigt, das sich auch im Erscheinungsbild deutlich von den bisherigen nicht sehr guten 11n-Vor-Standardprodukten aller Hersteller unterscheidet (kritischer Punkt ist nach wie vor die Antennen-Auslegung, so simpel wie physikalisch nicht umgehbare Punkte wie der Abstand zwischen den MIMO-Antennen).

Gehen Sie also davon aus, dass die Endgeräte, die Sie in den nächsten Wochen kaufen, zunehmend 11n-fähig sein werden (wir müssen diskutieren was das bedeutet).

Es ist sehr wahrscheinlich, dass im Enterprise-Bereich zusammen mit 802.11n auch der 802.11s-Standard umgesetzt wird. Auch dieser ist im Draft-Zustand, es sind deutlich mehr Fragen offen als

bei 11n, allerdings sind dies überwiegend Firmware- bzw. Software-Fragen. Mit 802.11s kommen Mesh-Netzwerke, die für viele Anwendungsbereiche einen großen Sprung in der Versorgbarkeit von schwierigen Flächen mit Netzwerk-Zugängen realisieren werden.

Die Vorteile der neuen Standards liegen auf der Hand, allerdings dürfen die damit verbundenen Fragen nicht übersehen werden:

- Hochwertige Anwendungen werden 40 MHz-Kanäle erfordern, dies wirft das bisherige Frequenzdesign völlig über den Haufen
- Die Access-Points erfordern in Zukunft eine Gigabit-Anbindung
- Der Wechsel in das 5 GHz-Spektrum ist unausweichlich
- Der Mischbetrieb aus a,b,g und n wirft einige Fragen auf, u.a. ob er überhaupt Sinn macht
- Die Versorgbarkeit der 11n-Access-Points mit Power-over-LAN ist nicht generell sicher gestellt
- 11n bringt offensichtlich ein Antennenproblem mit sich. Eine der Ursachen des mehr als schlechten Abschneidens vieler Vor-Standard-Produkte im Konsumer-Markt, deren Performance de facto niedriger war als die von guten g-Produkten, ist die Auslegung der Antennen

Wir analysieren für Sie: was bringen die neuen Technologien, wann sind sie einsatzbereit und was sollten Sie schon jetzt bei der Planung beachten

NT2) Microsoft, Voice, IP-Dienste
Microsoft wird mit seinem Einstieg in den Voice-Markt diesen Markt schnell und deutlich verändern. Viele Anwender unterschätzen diesen Einfluss bei Weitem, da sie zu sehr Einfluss mit Umsatz gleichsetzen. Viel wichtiger ist aber momentan die Technologie-Verschiebung, die Microsoft mit seiner Initiative auslöst. Wir haben eine große Analyse zu diesem Thema in Arbeit, können aber schon auf die folgenden Punkte hinweisen, die wir auf dem Netzwerk-Redesign-Forum mit Ihnen diskutieren müssen:

- Es wird zunehmend und relativ schnell Sprach- und Videokommunikationsbezogene Anwendungen auf den Endgeräten geben
- IP-Adressvergabe, DHCP, DNS müssen neu durchdacht werden, in deutlich mehr als 80% aller Fälle wird ein komplettes Redesign erforderlich sein
- VLAN, QoS, Benutzertrennung, NAC, alles ändert sich unter diesem Blickwinkel
- Der Einstieg von Microsoft steht im direkten Einklang mit den Aktivitäten von zum Beispiel Cisco und Siemens. Er bringt den schnellen Wechsel zu SIP als Basis-Standard für Sprach- und Multimedia-Kommunikation. Bereits jetzt ist sichtbar, dass die Verkäufe von Hybridanlagen in den USA viel schneller einbrechen als bisher angenommen. Dies liegt komplett auf der Linie unserer eigenen Prognose, die eine sehr schnelle Reduzierung von Hybrid-Lösungen auf Gateway- und Migrations-Aspekte sieht
- SIP in LAN und WAN: was bedeutet das, was zieht die Erlang(k)=1 Auslegung für Sprache nach sich. Wie muss Video kalkuliert werden?

Erwarten Sie hier mit Spannung unsere große Analyse zu dem Thema. Schon jetzt zeigt sich in unseren Untersuchungen die enorme Tragweite dieser Entwicklung. Hier wird kein Stein auf dem anderen bleiben, dieser Markt bricht sich total um. Was muss die Infrastruktur Netzwerk in nächster Zeit dafür leisten? Exklusiv für Sie auf dem Forum unsere Analyse zu diesem Thema.

NT3) IPv6
Die amerikanischen Behörden wechseln per Gesetz 2008 auf IPv6, Asien hat diesen Einstieg schon vollzogen, Ihr Unternehmen muss mit hoher Wahrscheinlichkeit seine IP-Dienste überarbeiten. Ist jetzt die Zeit für IPv6 gekommen, macht ein Redesign zum jetzigen Zeitpunkt Sinn ohne dabei gleich auf v6 zu gehen? Wie sieht ein Redesign der IP-Dienste überhaupt Sinnvollerweise aus? Welche Adressräume sollten wie genutzt werden, wie sieht ein standortübergreifendes Konzept aus?

Wir stellen unsere Überlegungen zu diesem Thema vor und diskutieren diese mit Ihnen.

Das soll als Ausblick auf das Forum für heute reichen. Es ist sehr viel in Bewegung, viele Analysen sind erforderlich und viele etablierte Lösungen müssen hinterfragt werden.

Das ComConsult Netzwerk Redesign-Forum greift die aktuellsten Trends und Themen auf, analysiert diese und bietet den Spielraum für Diskussion. Top-Referenten, Vorträge, Workshops und eine begleitende Ausstellung bilden den perfekten Rahmen, um sich kompakt auf den neuesten Stand der Technik zu bringen.

Zögern Sie nicht, sich hier rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu buchen.

Die Moderation übernimmt Dr. Jürgen Suppan. Er gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt.

Kongress

Netzwerk-Redesign Forum 2007
23.04. - 26.04.07
in Königswinter

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

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

Moderation: Dr. Jürgen Suppan
Preis: € 2.190,- zzgl. MwSt. mit Ein-Tages-Intensiv-Trainings/Workshops
€ 1.790,- zzgl. MwSt. ohne Ein-Tages-Intensiv-Trainings/Workshops

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

Security-Kongress des Jahres

IT-Sicherheits-Forum 2007

Die ComConsult Akademie veranstaltet in Zusammarbeit mit der GAI NetConsult unter der fachlichen Leitung von Dipl.-Inform. Detlef Weidenhammer vom 07.05. - 10.05.07 ihren Kongress „IT-Sicherheits-Forum 2007“ in Königswinter.

Das Programm besteht aus Seminaren, Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und interaktiver Erarbeitung von Schutzszenarien. Das Forum verbindet damit in idealer Weise die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Als Schwerpunktthemen sind in diesem Jahr vorgesehen:

- Welche neuen Bedrohungen erwarten uns in 2007?
- Windows Vista unter Sicherheitsaspekten
- Content-Security: Umgang mit gefährlichen Inhalten
- Sicherheit in Automatisierungs- und Prozesskontrollsystemen (SCADA)

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.

Einige Themenschwerpunkte des IT-Sicherheits-Forums im Detail:

- Welche neuen Bedrohungen erwarten uns in 2007?
  Obwohl das Jahr 2006 von Aufsehen erregenden Viren- oder Wurmepidemien weitgehend verschont blieb, hat sich doch einiges Neue bei den beobachteten Angriffen und Techniken getan. Die kommerziell motivierte Suche und Ausbeutung von Schwachstellen hat sich weiter fortgesetzt und eine besondere Gefahr stellt das starke Anwachsen von 0-Day Exploits dar. Auch MS-Office geriet erneut in den Fokus der Hacker und viele neue Schwachstellen tragen zur allgemeinen Verunsicherung bei. Die freie Verfügbarkeit von einfach zu bedienenden Tools zur Exploit-Entwicklung und automatisierten Verbreitung lassen auch für die Zukunft nichts Gutes erwarten. Im Forum werden die absehbaren Trends aufgezeigt und Gegenmaßnahmen vorgestellt.

- Windows Vista unter Sicherheitsaspekten
  Als wesentlicher Vorteil des neuen Windows-Betriebssystems wird zuvorderst die deutlich verbesserte Sicherheit genannt. Mit neuen Sicherheitsfunktionen wie User Account Control (UAC), BitLocker, Driver Signing oder Protected Mode des Internet Explorer 7 sollen die Nutzer besser geschützt werden. Erste Analysen zeigen aber, dass auch die neuen Features Schwachpunkte enthalten und zusätzliche Tools keineswegs vollständig ersetzen. Im Forum werden die Problembereiche aufgezeigt und Empfehlungen zur Einsatzplanung im Unternehmensumfeld gegeben.

- Sicherheit in Automatisierungs- und Prozesskontrollsystemen (SCADA)
  Die moderne IT-Technologie hat in den letzten Jahren auch ihren Weg in die klassische Automatisierungs- und Prozessleittechnik gefunden. Damit kommen die bekannten Hardware- und Software-Komponenten mit all ihren Tücken und Sicherheitsproblemen nun auch in sehr sensiblen Produktionsumgebungen und bei kritischen Infrastrukturen (KRITIS) zum Einsatz. Darüber hinaus wird auch die Vernetzung von einstmals weitgehend isoliert betriebenen Systemen mit anderen IT-Bereichen immer weiter vorangetrieben. Diese unaufhaltsame Entwicklung verlangt dringend nach erweiterten Sicherheitskonzepten, um solch wichtige Ressourcen gegen die neu auftretenden Bedrohungen angemessen abzusichern. Im Forum werden die Problembereiche aufgezeigt und Lösungen vorgestellt.

- Content-Security: Umgang mit gefährlichen Inhalten
  Nach der Zeit der Viren und Würmer stellen mittlerweile Trojaner die größte Gefahr im Internet dar. Kriminelle versuchen zunehmend durch den gezielten Einsatz von solch maßgeschneiderter Malware geheime Informationen von Einzelpersonen oder Unternehmen auszuspähen. Die Abwehr solcher Gefahren sollte schon an der Netzgrenze beginnen, deshalb kommt dem Einsatz von Content-Filtern eine große Bedeutung zu, auch wenn sie bei weitem nicht alle Schädlinge erkennen können. Ein weiteres Problem im Unternehmensbereich stellt die zunehmende Nutzung von Anwendungen dar, die zur Umgehung der Firewallkontrollen diese „durchtunneln“. Nur ein Filter, der auf Anwendungsebene agiert, hat eine Chance dieses zu erkennen und zu verhindern. Das Forum beleuchtet Angriffstechniken / Gegenmaßnahmen und zeichnet exemplarisch einige bekannt gewordene Vorfälle nach.

Neben diesen Schwerpunkten sind weitere Beiträge zu folgenden Themen geplant:

- Praxiserfahrungen aus ISMS-Projekten
- Besondere Aspekte der Notfallplanung
- Erstellung und Betrieb von sicheren Webanwendungen
- Einschätzungen zu aktuellen Standards im Sicherheitsbereich
- Datenschutzaspekte bei VoIP
- Compliance / Risk Management
- Bluetooth-Security
- Praxis-Workshops

Am 1. Tag ist geplant, die folgenden Seminare jeweils mit Live-Demos durchzuführen:

1. Security-Auditing: Von Pentests bis zu Compliance-Analysen
2. Prozessorientiertes IT-Sicherheitsmanagement mit ITIL
3. Umsetzung einer sicheren Netzzugangskontrolle

Am 3. Tag werden in parallelen Sessions stark praxisorientierte Workshops durchgeführt. Dazu gehören moderierte Produktvergleiche ebenso wie die gemeinsame Erarbeitung von Lösungsszenarien (u.a. für Prozesskontrollsysteme, Sicheres Netzwerk-Management, VoIP-Security).

Anmeldungen Kongresse Frühjahr 2007

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2007

☐ Ich buche den Kongress
Netzwerk-Redesign Forum 2007
vom 23.04. - 26.04.07 in Königswinter
inkl. Intensiv-Training am ersten Tag
zum Preis von € 2.190,- zzgl. MwSt.

☐ vom 24.04. - 26.04.07 in Königswinter
ohne Intensiv-Training am ersten Tag
zum Preis von € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult IT-Sicherheits-Forum 2007

☐ Ich buche den Kongress
ComConsult
IT-Sicherheits-Forum 2007
vom 07.05. - 10.05.07 in Königswinter
inkl. Tutorium am ersten Tag
zum Preis von € 1.990,-* zzgl. MwSt.

☐ vom 08.05. - 10.05.07 in Königswinter
ohne Tutorium am ersten Tag
zum Preis von € 1.590,-* zzgl. MwSt.

☐ mit Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
zum Sonderpreis von nur € 338,-

Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

*gültig bis 15.02.07

Nur noch bis zum 15.02.2007 Frühbucher-Rabatt

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Stellenanzeige

Stellenangebot: Netzwerk- und System-Spezialist

ComConsult-Research/ComConsult Technologie-Information GmbH sucht für ihren Labor- und Vortragsbereich einen

Netzwerk- und System-Spezialisten

Wir erwarten folgende Qualifikation:

- Gute bis sehr gute Kenntnisse in aktuellen Netzwerk-Technologien, insbesondere Ethernet, TCP/IP, Wireless LAN
- Gute Kenntnisse in Konfiguration und Betrieb aktiver Netzwerkkomponenten (Cisco, Enterasys, Extreme)
- Gute bis sehr gute Kenntnisse in Windows- und Linuxbasierten Betriebssystemen
- Gute Kenntnisse in Voice over IP, SIP und Telekommunikation

Die Stelle umfasst folgende Tätigkeiten:

- Unterstützung beim Betrieb der hausinternen Netzwerk- und Systemlandschaft
- Eigenständige Durchführung von Produkttests und Analysen (nächste Themen: Mitwirkung beim SIP/Asterisk und HiPath 8000-Test)
- Vorbereitung und Durchführung von Vorträgen und Seminaren
- Verfassen von Artikeln und Reports zu aktuellen Themen
- Mitarbeit bei der Vermarktung und Positionierung unserer Produkte

Wir unterstützen unsere Kunden bei der Auswahl von Technologien und Produkten im Netzwerk- und Systembereich. Unser Ziel ist es, Neuentwicklungen frühzeitig zu bewerten, auf Risiken und Chancen neuer Techniken rechtzeitig hinzuweisen. Sie sollten daher aufgeschlossen gegenüber neuen Technologien sein und den permanenten Weiterentwicklungen im Markt mit Spannung und Neugierde entgegen sehen. Dementsprechend ist diese Stelle mit permanenter Weiterbildung verbunden. Sie arbeiten eng mit einem Team ausgewiesener Experten, eine ausgeprägte Teamfähigkeit ist daher unverzichtbar. Erfahrungen aus der Praxis sind von Vorteil.

Ihre Bewerbung richten Sie bitte an:

ComConsult Technologie Information GmbH
Laborleiter
Dipl.-Math. Cornelius Höchel-Winter
Pascalstr. 25 - 52076 Aachen

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

ComConsult Technologie Information

ComConsult Research

Zweitthema

Network Access Control NAC - Die Grundzüge einer neuen Technologie

Fortsetzung von Seite 1

Markus Nispel ist viele Jahre bei Enterasys Networks (ehemals Cabletron Systems) in den Bereichen Post- und Pre-Sales tätig gewesen. Hierzu gehört bis heute auch die Betreuung von Key Accounts wie SAP AG und Deutsche Bahn AG. Weiterhin ist er als „Director of Technology“ für den Chief Technology Officer, CTO von Enterasys Networks tätig, um Neuentwicklungen im Produktportfolio von Enterasys Networks voranzutreiben.

In einer Studie aus dem Januar 2006 erwartet Infonetics ein weltweites Umsatzwachstum von $323 Millionen in 2005 auf $3.9 Milliarden im Jahr 2008 (> 1100% Wachstum), wobei das meiste Wachstum durch Infrastrukturkomponenten wie Switches, VPN Konzentratoren, Wireless Switches etc. realisiert wird - siehe auch http://www.infonetics.com/resources/purple.shtml?ms06.nac.nr.shtml.

1. Definition von NAC

Im Allgemeinen kann man NAC als eine benutzerfokussierte Technologie beschreiben, die ein genutztes Endgerät autorisiert und Zugriff auf Ressourcen gewährt auf der Basis der Authentisierung der Identität des entsprechenden Benutzers (oder/und Gerätes) sowie auf dem Status des Gerätes im Hinblick auf sicherheitsrelevante Parameter und Einstellungen: die Compliance mit entsprechenden Unternehmensvorgaben. Diese Parameter werden im so genannten Pre-Connect Assessment ermittelt, d.h. vor Anschluss an die Infrastruktur. Es sollte aber auch dann im laufenden Betrieb eine Überprüfung erfolgen, welche dann als Post-Connect Assessment bezeichnet wird. Teilweise wird auf den einen oder anderen Baustein im Rahmen einer Implementierung auch verzichtet - je nach Kundenanforderung. Ein Prozess zur Wiederherstellung der Compliance, der sog. Remediation, ist hier ebenfalls enthalten. Die gilt für alle Endgeräte und Nutzer am Netz, d.h. eigene Mitarbeiter, Partner, Gäste, Kunden und sonstige Geräte wie Drucker, Videokameras etc.

NAC ist aber auch nicht das Allheilmittel gegen beliebige Sicherheitsprobleme. Insbesondere falsches Nutzerverhalten und Angriffe auf Applikationsebene können mittels NAC kaum erkannt werden, es sei denn, man setzt intensiv auch Post-Connect Assessment Techniken ein. (http://media.godashboard.com/CMP/Excerpt_nwcanl06_nac.pdf)

2. Herausforderungen für ein Unternehmen

NAC ist insbesondere eine prozessuale und organisatorische Herausforderung für größere Unternehmen. Um die gewünschten Effekte zu erzielen, müssen die Netzwerk-, die Security- und die Desktopmanagementabteilung eng verzahnt miteinander arbeiten. In der Konzeptionsphase aber auch und insbesondere im Betrieb: Die Netzwerkabteilung muss eine entsprechende Authentifizierung der Endgeräte und Nutzer durchführen. Dazu muss Zugriff auf Directory Services erfolgen. Die Sicherheitsabteilung hat die Compliance Vorgaben zu machen und zu kommunizieren. Die Desktopmanagementabteilung muss die Vorgaben prüfen und in geeigneter Form der Netzwerkabteilung als zusätzlichen Parameter bei der Authentifizierungsphase mitteilen. Die Security Abteilung hat zusammen mit der Netzwerkabteilung zu definieren, was bei einem non-compliant Endsystem zu tun ist, welche Zugriffe noch möglich sein sollen und in welchen Schritten das Problem zu beheben ist.

All diese Schritte sind notwendig, um NAC effektiv einzusetzen. Hinzu kommt die entscheidende Frage zur Auswahl der adäquaten Technik. Da sich der Markt noch am Anfang befindet, konkurrieren viele unterschiedliche Ansätze miteinander wobei sich am Horizont aber schon auch eine Standardlösung abzeichnet. Je nach Unternehmen kann auf diese gewartet werden oder es müssen sinnvolle Zwischenschritte unternommen werden, die zum gewünschten Ziel führen.

Im Folgenden soll insbesondere auf das Thema Technologie und Abhängigkeiten bei einer NAC Implementierung eingegangen werden. Die verschiedensten Ansätze werden beleuchtet und Vor- bzw. Nachteile dargestellt.

3. Der Prozess „NAC“

Es gibt hier verschiedenste Modelle zur Darstellung eines NAC Prozesses. Generell ist die folgende Einteilung sinnvoll (lt. Gartner):

- Policy - die Erstellung einer Policy ist notwendig, um die Konfigurationseinstellungen, die Zugriffsrechte und die Authentisierung sowie die Korrektur und Quarantäne Einstellungen zu regeln.
- Baseline - erkennt den Security Status bei bzw. vor Anschluss an die Netzinfrastruktur
- Access Control - die Zuweisung von Zugriffsrechten aus dem Vergleich von Policy und Baseline
- Mitigation - bei einer Diskrepanz und limitierten Zugriffsrechten (Quarantäne) sollte hier eine vollautomatische Beseitigung der Probleme via Softwareverteilung, Patchmanagement und Konfigurationsmanagement erfolgen
- Monitor - es muss laufend überprüft werden, ob der Anfangsstatus sich nicht verändert
- Contain - falls dies doch geschieht, muss reaktiv eine erneute Quarantäne erfolgen können
- Maintain - es muss eine laufende Anpassung und Optimierung erfolgen

Wie zuvor erwähnt, sind hier die Workflows und die Organisation eines Unternehmens entsprechend anzupassen bzw. zu optimieren.

4. Lösungsansätze

4.1 Die großen Frameworks - das Endziel

Zunächst gestartet, um die Integrität eines Endsystems in Bezug auf Hardware- und Softwarekonfiguration sicherzustellen (und damit einen Grossteil bestehender Host IPS und Personal Firewall Ansätze zu ersetzen), können diese Ansätze optimal durch bestehende API´s auch zur Kommunikation des Security Status eines Endsystems in einer NAC Umgebung genutzt werden.

Die IETF teilt die Funktionen wie in Abbildung 1 ein.

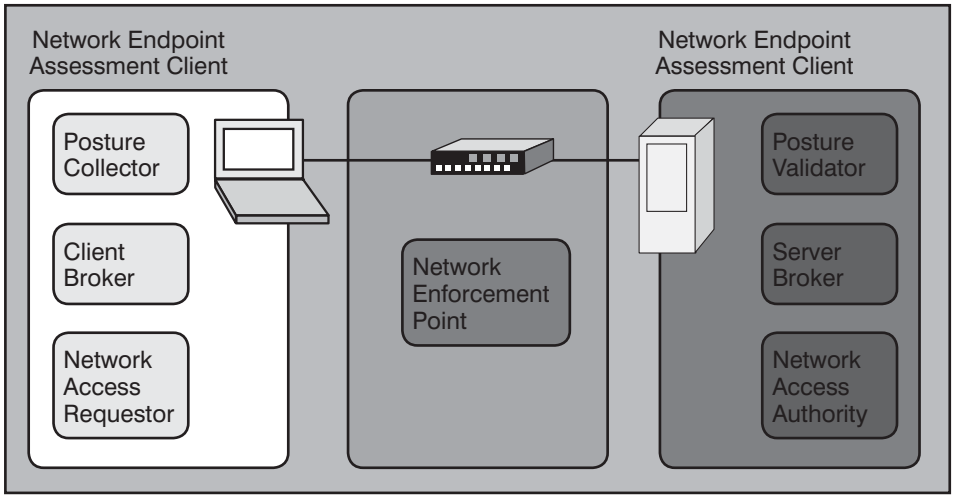


Abbildung 1: Funktionseinteilung der IETF

Der „Agent“ auf dem Endsystem ist typischerweise mehrteilig - der Posture Collector überprüft einzelne Einstellungen (je nach Hersteller des Kollektors) wie z.B. Patchlevel, Antivirus Status, Personal Firewall Einstellungen etc. und gibt diese an den Client Broker weiter, dessen API von verschiedenen Posture Kollektoren genutzt werden kann. Der Client Broker wiederum gibt diese Information an den Network Access Requestor weiter, der neben Authentifizierung auch den Security Status an den die Serverseite leitet. Typisch für einen Network Access Requestor sind 802.1X Supplicants oder IPSec Clients.

Beim Network Enforcement Point handelt es sich typischerweise um Switches, Router, Access Points, Firewalls und IPS Systeme oder VPN Konzentratoren.

Auf der Serverseite werden die Komponenten der Client Seite widergespiegelt in Form der Network Access Authority, die typischerweise einem Radius Server bzw. einem Policy Server entspricht, der den Network Enforcement steuern kann und dem Server Broker (einem Stück Middleware wie auch der Client Broker), der wiederum die verschiedenen Posture Validatoren anspricht.

Für agentenbasierte Lösungen werden diese Lösungen in den nächsten 2 bis 5 Jahren wohl die dominierende Position einnehmen.

4.1.1 Microsoft NAP

Die Microsoft NAP Network Access Protection Lösung, die mit MS Vista und Longhorn Server Einzug hält, wird wohl erst ab Anfang 2008 für „General Deployments“ bereitstehen. Die Beta Tests und Early Adaptor Implementierungen sind für 2007 geplant bzw. schon am Laufen. Es wird auch einen NAP Client für Windows XP geben, das wird jedoch die minimale Anforderung für die Kunden sein. Der NAP Client wird dann DHCP, VPN und 802.1X Enforcement unterstützen.

Folgendes Mapping gilt für NAP in Bezug auf das IETF Modell:

Posture Collector - System Health Agent (SHA)
Client Broker - NAP Agent (Quarantine Agent QA)
Network Access Requestor - NAP Enforcement Client (Quarantine Enforcement Client QEC)
Policy Enforcement Point - NAP Enforcement Server (Quarantine Server QS)
Network Access Authority - Network Policy Server (NPS)
Server Broker - Network Policy Administration Server
Posture Validator - System Health Validator (SHV)

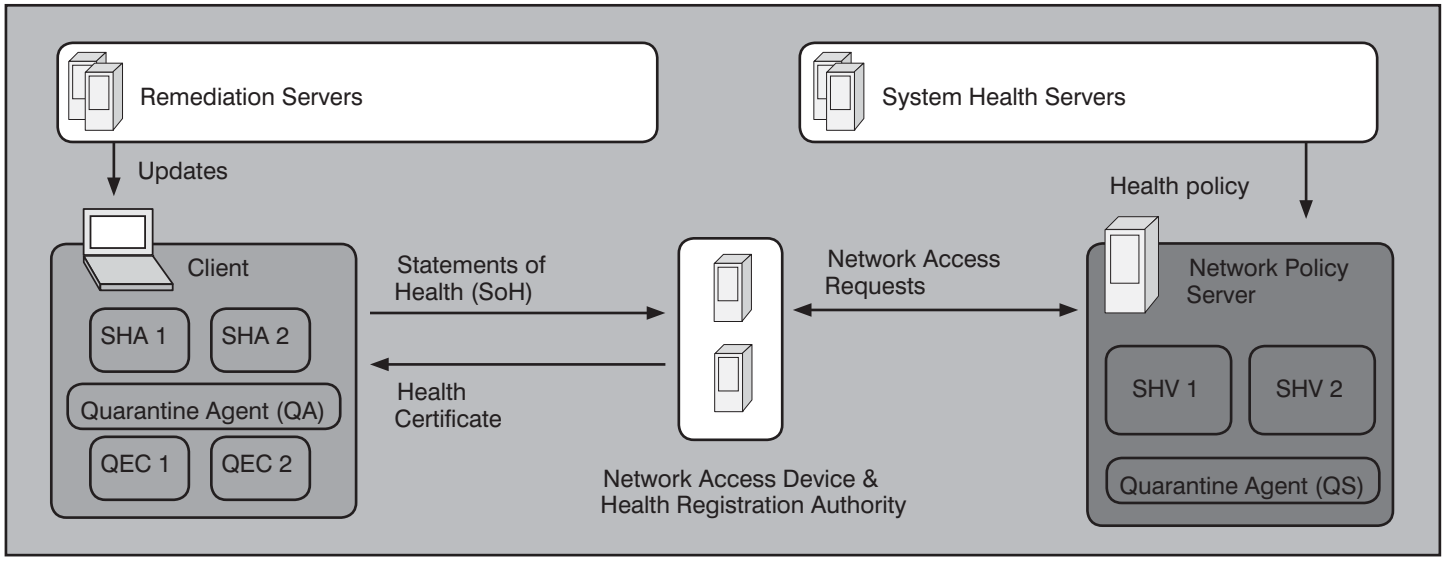


Abbildung 2: Steuerung via Radius Server (Quelle: Microsoft)

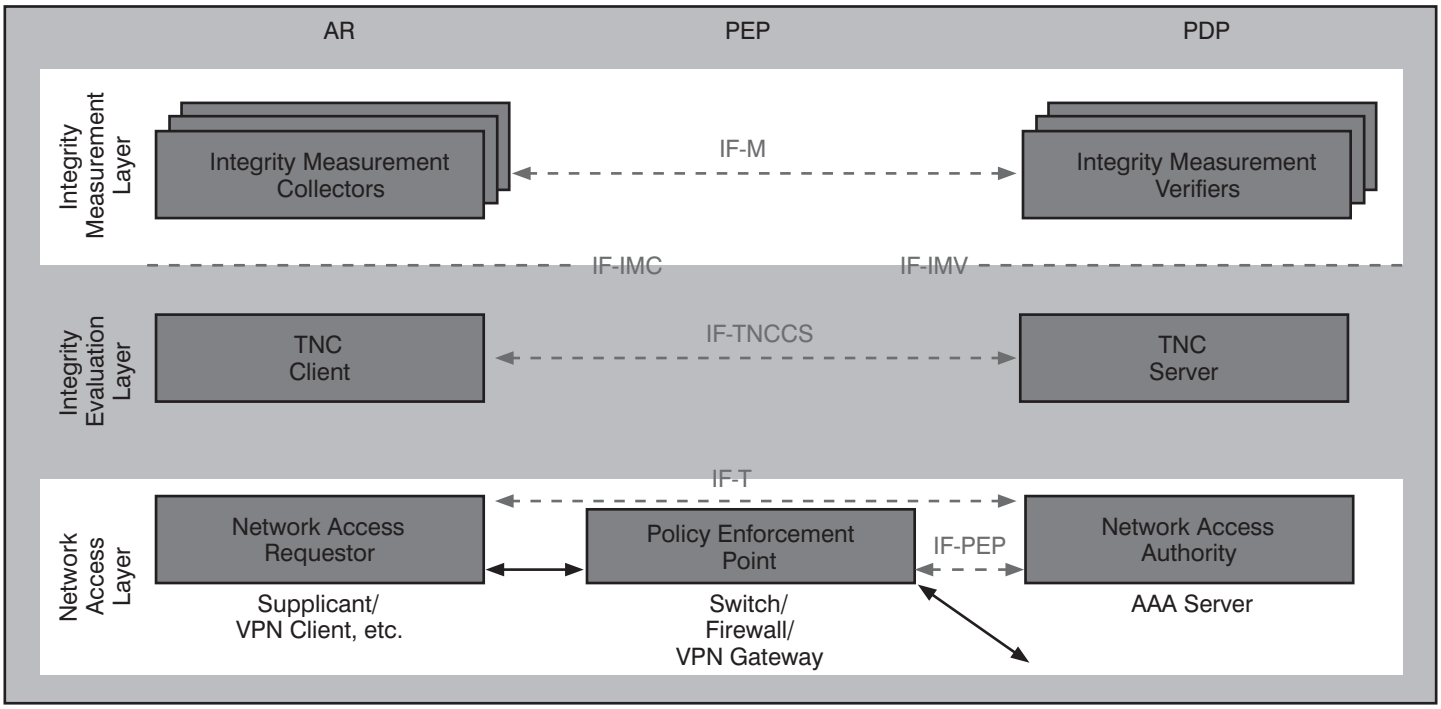


Abbildung 3: TNC-SG 1.1 Spezifikation (Quelle: TNC)

Der Enforcement Point kann aber auch in der Netzwerkinfrastruktur liegen, die Steuerung erfolgt dann via einem Radius Server (siehe Abbildung 2).

4.1.2 Trusted Computing Group TCG - TNC

Da der Endgerätemarkt nicht nur aus Microsoft Produkten besteht, ist insbesondere hier ein Standard notwendig, der sich mit der TCG und deren Sub-Group TNC-SG Trusted Network Connect abzeichnet. Vereinzelt sind auch schon Produkte zu finden, die diese Spezifikation unterstützen. Ein großer Durchbruch ist aber in 2007 zumindest für TNC noch nicht zu sehen, obwohl schon mehr als 160 Unternehmen dort Mitglied sind. Das Modell der TNC-SG 1.1 Spezifikation sieht auch wiederum sehr dem MS NAP Konzept ähnlich (siehe Abbildung 3)

Posture Collector und Validator entsprechen jetzt den Integrity Measurement Collectors und Verifiers, die Client und Server Broker sind die eigentlichen TNC Clients und Server, die Network Access Requestor, Network Access Authority und Policy Enforcement Point Instanzen bleiben identisch.

4.1.3 Cisco CNAC

CNAC besteht prinzipiell aus ähnlichen Komponenten wie die zuvor besprochenen Frameworks - auf der Client Seite primär aus dem CTA Cisco Trust Agent, der als Network Access Requestor, Client Broker und in Teilen als Posture Collector (für OS Patch und Hotfix Überprüfung) fungiert. Er stellt auch eine Cisco eigene API und ein Skripting Interface für externe Posture Collectoren bereit (und nebenbei kann der CSA Cisco Security Agent als Enforcer und Posture Collector genutzt werden). Auf der Serverseite besteht CNAC aus dem Cisco ACS Access Control Server, der als Radius Server der Network Access Authority und dem Server Broker entspricht. Cisco setzt im CNAC Programm auf die Integration von Partnern für den Posture Check, der mittels der Cisco proprietären Protokolle Host Credential Authorization Protocol (HCAP) und Generic Authorization Message Exchange (GAME) erfolgen kann. GAME ist eine SAML (Security Assertion Markup Language) basierte Sprache für die Kommunikation mit Audit Servern, HCAP ermöglicht die Überprüfung der Security Posture auf den jeweiligen Policy Servern z.B. der Anti Virus Hersteller, die im CNAC Programm teilnehmen.

Nachdem CNAC Phase 2 lange hat auf sich warten lassen (und damit neben Routern auch Switches mit 802.1X unterstützt werden), hat Cisco realisieren müssen, dass die Kundenbasis mit ihren Infrastruktur-Upgrades nicht für CNAC bereit ist. Und schnell wurde ein Unternehmen gekauft (Perfigo), um das Produkt namens CleanAccess anzubieten. Es gehört zur Klasse der Out of Band Appliances (mit Inband Option für geringe Portdichten/Geschwindigkeiten) - siehe folgende Kapitel. Aktuell ist noch nicht zu erkennen, wie Clean Access und CNAC zusammenkommen sollen.

Mit Microsoft NAP stellt sich Microsoft neben dem Voice VOIP Geschäft auch im Security Umfeld als Wettbewerber von Cisco auf. Das wurde erkannt und schnellstens eine Kooperation vereinbart, die effektiv dazu führt, dass der CTA für Microsoft basierte Endsysteme verschwinden wird und nur EAP-FAST sowie EAPoUDP als proprietäre Fragmente auf dem Desktop übrig bleiben und in den NAP Agent integriert werden.

4.1.4 Das zukünftige Zusammenspiel in heterogenen Umgebungen

Auf der Desktop Ebene wird Microsoft mit dem NAP Agent wohl eine maßgebliche Rolle spielen - in Bezug auf Sicherheit zieht Microsoft hier die Daumenschrauben stark (vielleicht auch zu stark ?) an. Die Akzeptanz der TNC Implementierungen wird in der non-Microsoft Welt groß sein, für Microsoft basierte Endsysteme bleibt dies abzuwarten. Eine Integration der verschiedenen Systeme ist möglich auf der Serverseite - hier müssen intelligente Network Access Authority Server erkennen, welche Clients installiert sind (oder Client-Less gearbeitet wird) und auf dieser Basis muss eine Umleitung an den entsprechenden (Network Access Authority) Server erfolgen. Enterasys geht mit Enterasys Sentinel™ diesen Weg des intelligenten Radius Proxies und Brokers, der diese Integration übernehmen kann. Auf dem Desktop muss sich der Kunde für jeweils einen Agenten und eine Technologie entscheiden.

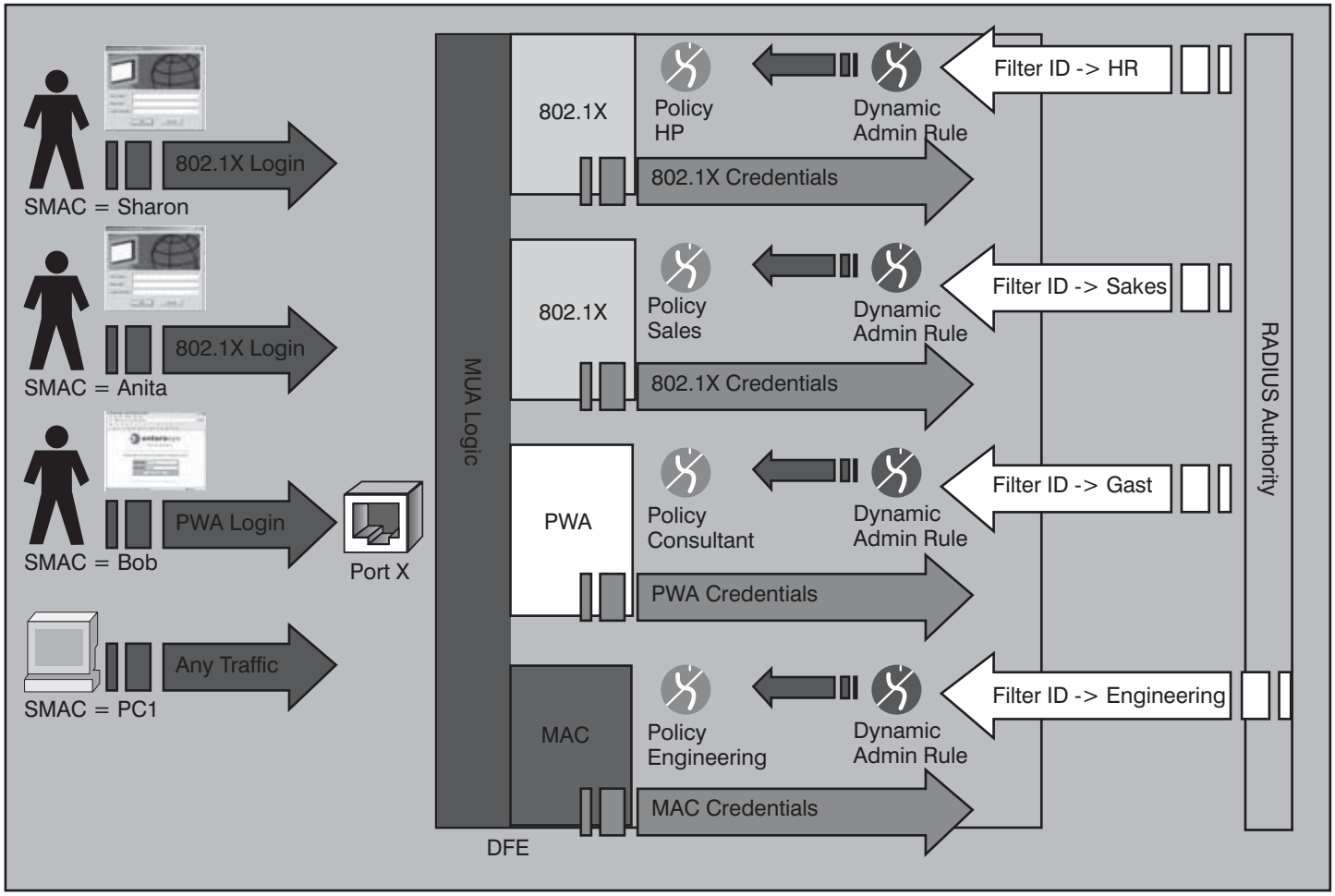


Abbildung 4: Policy Vergabe

4.2 Policy Enforcement Points - Optionen

4.2.1 Switch based

Die optimale Lösung für NAC im LAN ist die Implementierung von Access Switches, die eine entsprechende Authentifizierung via 802.1X und eine Zuordnung von Policies (via VLAN aber besser mit ACL und Rate Limits) unterstützt. Insbesondere aber auch in einer heterogenen Umgebung mit non-802.1X Endgeräten und mehreren Geräten pro Switch Port (z.b. Voice over IP Phones und ein PC in Reihe geschaltet) sind hier mehr Optionen notwendig. Dies gilt auch für Migrationen (nicht alle Access Switches können gleichzeitig getauscht werden) und bei der Verwendung von Fibre to the Office (Kabelkanal- oder andere Mini Switches setzen dann auf Kupfer um, können keine Authentisierung oder nur mit erheblichem finanziellen und verwaltungstechnischem Aufwand) ein entscheidender Faktor. Wenn man Authentisierung einführen möchte, stellt sich zunächst die Frage nach der Art und Weise des Verfahrens. Es gibt mehrere Möglichkeiten, dies zu tun. Hier ist man sehr abhängig vom verwendeten Endsystem:

- **802.1X** für eigene PCs und Laptops, in Zukunft teilweise auch IP Phones ist die präferierte Lösung
- **MAC Adresse** für Drucker, IP Phones und andere Maschinen am Netz (Sicherheitskameras, Produktionssteuerungen, Sensoren etc.)
- **Web Portal** für Gäste, Consultants, Service Techniker
- **Default** Eigenschaften z.B. für TFTP/ Bootp, damit Diskless Stationen booten

Ein Switch muss optimalerweise alle Verfahren gleichzeitig pro Port unterstützen, damit man nicht den Administrationsaufwand unnötig erhöht (sonst muss bei jedem Umzug ja das Authentisierungsverfahren angepasst werden). Bei der Authentisierung verschiedener Benutzer/ Geräte gleichzeitig an einem Port ist natürlich davon auszugehen, dass an diesem Port dann auch unterschiedliche Gruppen-Regeln je nach Benutzer und Gerät spezifisch und gleichzeitig vorhanden sein müssen. Der PC soll z.B. andere Regeln bekommen wie das IP Phone am selben Port. Ein Gast soll andere Regeln haben wie ein eigener Mitarbeiter etc. d.h. nach erfolgreicher Authentisierung muss eine Policy Vergabe pro Benutzer/Gerät erfolgen. (siehe Abbildung 4)

Hierbei können mehrere „User“ pro Port mit beliebigen Authentisierungsverfahren zu völlig unterschiedlichen Policies dynamisch zugeordnet werden. Ein weiteres Augenmerk sollte auf die Art der Policies gelegt werden: Oft werden nur einfache VLAN Policies unterstützt, innerhalb eines VLANs gibt es aber gar keine Kontrolle:

- Was passiert nun, wenn jemand einen unautorisierten DHCP Server an das VLAN anschließt (und sich mit passenden Credentials anmeldet)?
- Wie unterscheide ich hier bei einem Softphone (auf dem PC) zwischen VOIP und Datenverkehr?
- Wie kann ich eine Wurmausbreitung innerhalb eines VLANs stoppen?

Die Antwort liegt in Port Policies (ACLs und QoS auf Layer 2-4), die auch zwischen Ports im gleichen VLAN greifen und auch Informationen von Layer 2 (VLAN/ MAC Adresse) bis Layer 4 (Applikation -

http, Email, VOIP) mit einbeziehen. (siehe Abbildung 5)

Hinzu kommt dann die Verifizierung des Endsystemstatus während der Authentisierung. Beispielhaft hierzu die Schritte bei einer Enterasys Secure Networks™ Lösung (siehe Abbildung 6).

4.2.2 Appliance based

Um schneller eine NAC Lösung zu implementieren, wird heute verstärkt das Augenmerk auf Appliances gelegt, die oft

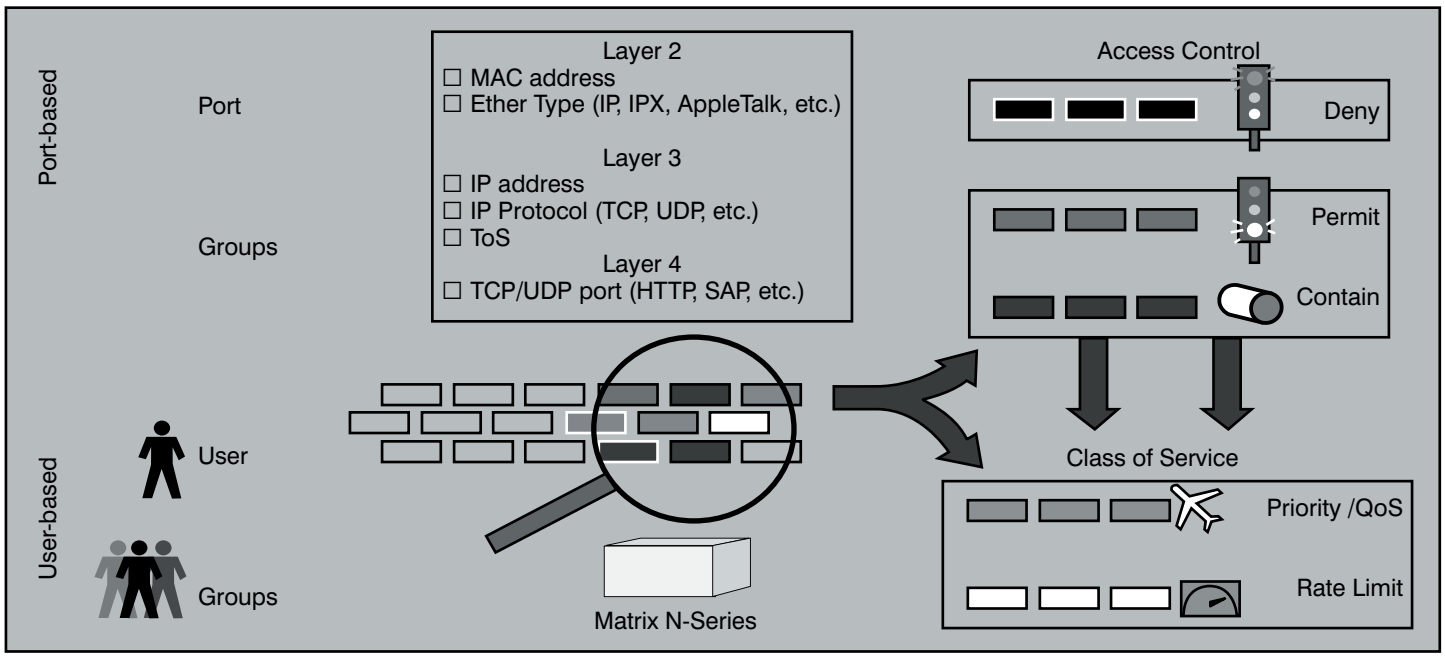


Abbildung 5:

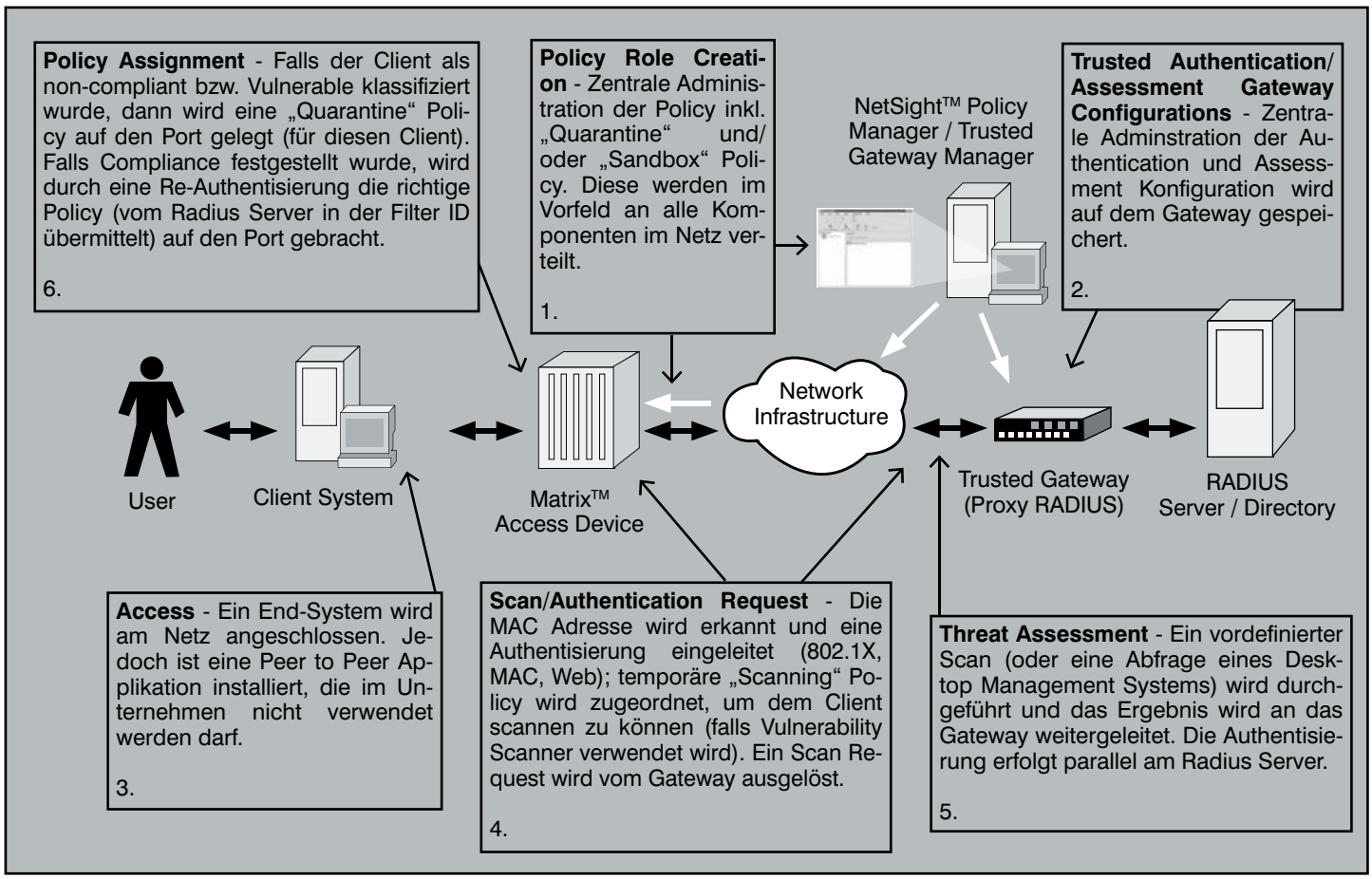


Abbildung 6: Switch based NAC - ein Beispiel

eine Übergangslösung zu einer Switch basierten NAC Lösung darstellen. Die Access Switches können zunächst weitergenutzt werden, auch wenn sie keine Authentifizierung und Policy Verfahren unterstützen. In sehr heterogenen Umgebungen mit relativ alten Switches ist dies ein gangbarer Weg.

4.2.2.1 Inband Appliances

Diese Appliances sind typischerweise eine Erweiterung einer Switch basierten Lösung mit der Unterstützung von mehreren hundert bis mehreren tausend Geräten pro Port, die mit unterschiedlichsten Authentifizierungsverfahren und Policies autorisiert werden können. Zusätzlich sind oft Windows Login Snooping Verfahren (Kerberos Snooping etc) zu finden, die eine User zu IP Adressen Verbindung herstellen.

Eine Implementierung im so genannten Distribution Layer eines Netzwerkdesigns ist der optimale Ort für eine Inband Appliance, die auch hinter einem WLAN Switch oder VPN Konzentrator installiert werden kann. (siehe Abbildung 7)

4.2.2.2 Out of band Appliances

Im Gegensatz zu den Inband Appliances stehen die out of band Appliances für den normaler Verkehr nicht im Datenpfad - jedoch bei der Authentifizierung, im Assessment Prozess und auch im Quarantäne Fall. Es gibt zwar auch Lösungen, die hier out of band arbeiten, das ist jedoch eher die Ausnahme als die Regel.

Dieser Ansatz erscheint zunächst sehr attraktiv, er hat aber auch seine Tücken - insbesondere in den Bereichen

- Erkennung neuer Endsysteme
- Rekonfiguration der Access Switches im Assessment und Quarantäne Fall
- Granularität im Assessment und Quarantäne Fall

Diese Probleme können zwar durch das Einschalten einer 802.1X Authentifizierung am Access Switch umgangen werden, dann entspricht das Ganze aber eher einer Switch based NAC Lösung und die Appliance ist kaum noch erforderlich. Die Erkennung erfolgt typischerweise durch SNMP Traps für neue MAC Adressen (die jeder Hersteller anders implementiert) oder durch das regelmäßige Pollen von Source Address Tabellen oder Router ARP Caches in den verschiedenen Netzkomponenten - was auch sehr unzuverlässig und mit Verzögerungen verbunden ist. Auch sind die Access Switches hier mit einer Reihe von Quarantäne VLANs zu konfigurieren, was wiederum einen höheren administrativen Aufwand bedeutet. Die automatische Rekonfiguration eines Port VLANs durch die Appliance ist dann auch oft wieder herstellerspezifisch. Dies zeigt sich dann auch in der Granularität der Antwort (Port VLAN Änderung und ACL, die wiederum herstellerspezifisch ist) und es ist fast unmöglich in einer VOIP Umgebung (PC & IP Phone am selben Switch Port). (siehe Abbildung 8)

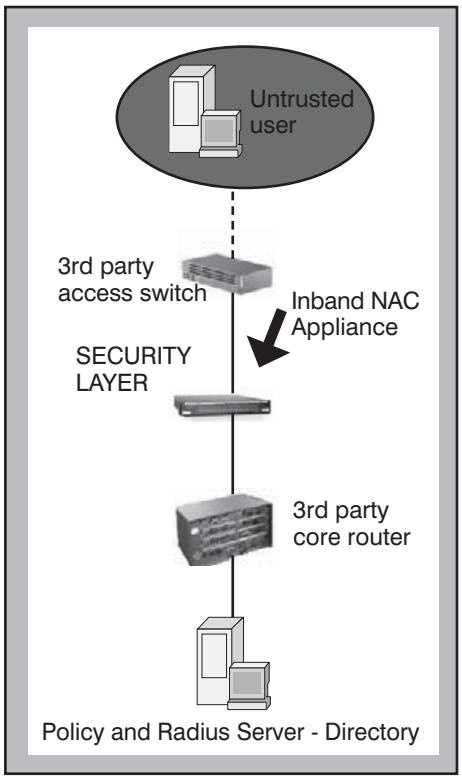


Abbildung 7: Inband Appliances

4.2.3 Software based

Ein Enforcement auf dem Agent des Clients bietet sehr präzise Möglichkeiten zur Steuerung im Quarantäne Fall. Die neuen Frameworks werden hier gute Möglichkeiten bieten. Es gibt auch heute schon eine Reihe von Personal Firewall und Host Intrusion Prevention Herstellern, die sich seit längerem dieser Thematik widmen. Checkpoint Integrity oder auch Symantec, um nur 2 bekannte zu nennen. Diese Lösungen können auch aber wiederum mit netzwerkbasierten Lösungen kombiniert werden können.

4.3 Pre Connect vs. Post Connect Assessment

4.3.1 Pre Connect Assessment Optionen

4.3.1.1 Network based

Hier werden die typischen Netzwerkscan Produkte wie Nessus, Tenable, eEye, Qualys, Rapid7 etc. eingesetzt und mit den NAC Appliances meist auf proprietäre Weise verknüpft. Mit entsprechenden Credentials auf dem Endsystem sind hier auch tiefere Analysen möglich wie File System, Anti Virus und Registry Prüfungen. Diese Produkte prüfen typischerweise beliebige Betriebssysteme.

Die Vorteile sind hier

- Kein Agent notwendig
  - Beliebige Endsysteme integrierbar (kein OS Support Problem)
  - Hersteller-neutral
  - Agent auf Systemen, die nicht unter

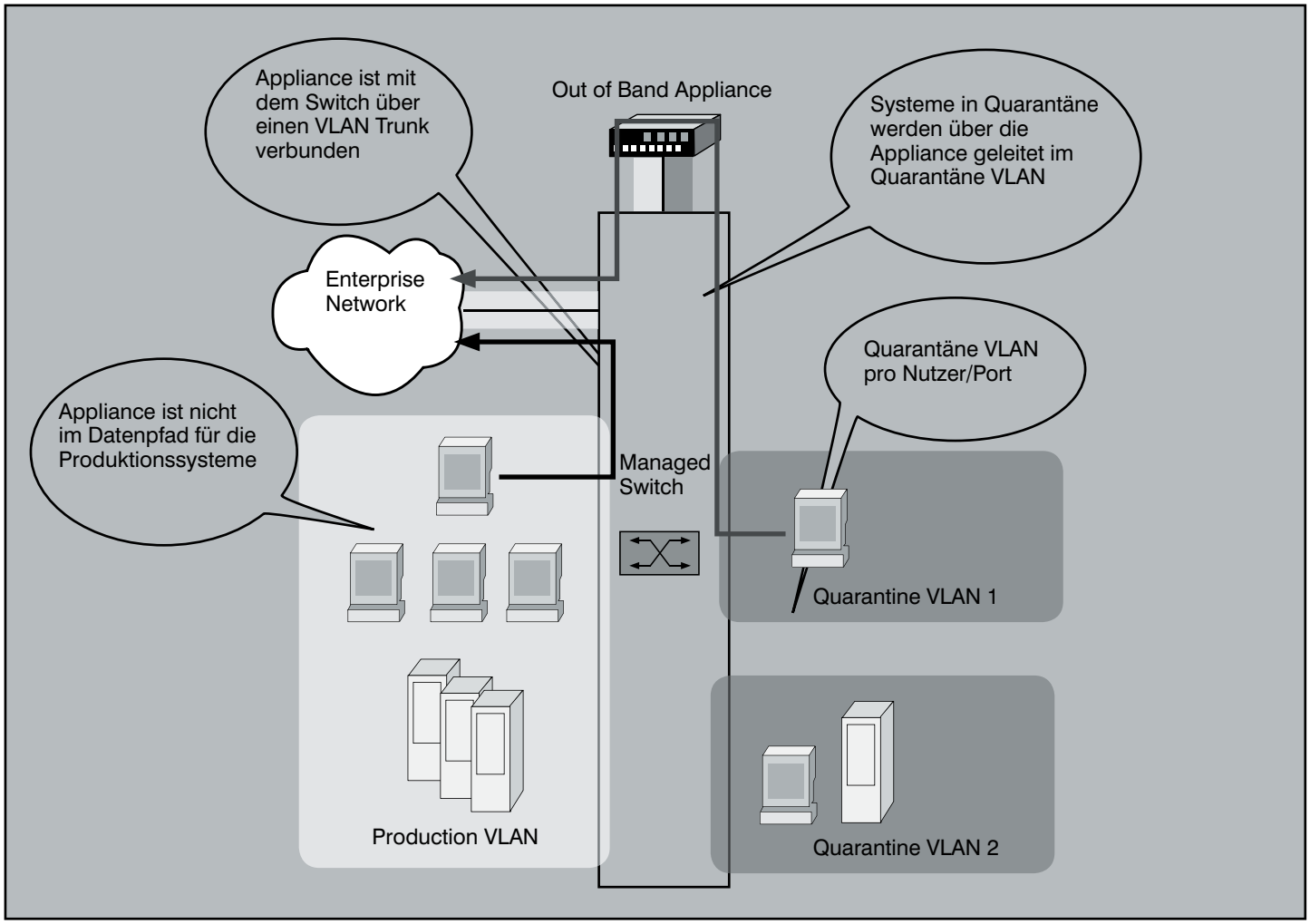


Abbildung 8: Network based PEP - Appliances

eigener Hoheit stehen und kein
  - Admin Account vorhanden ist, unmöglich!
- Verringert das Risiko durch neue Benutzer, Besucher etc.
- Zentral verwaltbar, wenige Komponenten notwendig
- Ist transparent für sichere Endgeräte
- Kann mit beliebigen Vulnerability Assessment und auch Desktop Management Systemen gekoppelt werden
- Kann komplementär zu agentenbasierten Lösungen eingesetzt werden

Der Nachteil ist die limitierte Möglichkeit zur Überprüfung von Funktionen auf dem Client, wenn keine Credentials zur Verfügung stehen.

4.3.1.2 Light Agent based

Heute gibt es hier mehrere Ansätze, die wiederum mit permanenten (zum reinen Baselining, ohne Enforcement Option) oder auch mit temporären Agenten (typisch Java Applets) arbeiten. Diese sind oft Windows zentriert.

4.3.1.3 Fat Agent based

Das sind die schon beschriebenen Framework Agenten. Sie kombinieren das Baselining mit HIPS und PFW Funktionen für das Enforcement. Die Vorteile sind die sehr gute Kontrolle des Endsystems (mit der o.g. Steuerung sind beliebige Programme auf dem Endsystem kontrollierbar) und die Tatsache, dass keine Verzögerung durch Scans etc. auf dem Endsystem (der Agent hat schon im Vorfeld den Status des Endsystems ermittelt und überträgt diesen einfach mit der Authentisierung mit).

Aber auch die bestehenden Desktop-, Patch- und Konfigurationsmanagement Agenten wie die von Altiris, Patchlink, IBM, CA können hier mit genutzt werden. Damit entfällt der Aufwand der Installation eines weiteren Agenten.

Die Nachteile dieser Lösung sind:

- Betriebssystem-spezifisch
  Heute primär nur in der Microsoft Welt verfügbar
  Linux eher noch unterrepräsentiert
  Was ist mit Symbian, Palm, PocketPC etc.?
- Agenten-Verwaltung
  Erhöhter Betriebsaufwand, schwierigeres Troubleshooting
  Kosten pro Agent
  Einfluss des Agenten auf die Endsystem Performance
- Fremdsysteme
  Nicht auf Fremdsystemen (Gäste, Service Techniker, Anlagenkontroller, Phones) installierbar
- Falls Agent gehackt wird, ist eine beliebige Manipulation möglich

4.3.2 Post Connect Assessment

Die Überprüfung des Clients vor Anschluss an die Infrastruktur und auch dessen regelmäßige Prüfung löst nur einen Teil des Sicherheitsproblems. Ein völlig konformes Endsystem kann dennoch nicht autorisierte Aktionen in der Intrastruktur vornehmen. Diese müssen auch erkannt werden und im gleichen Prozess enden wie eine Identifikation eines Problems bei/vor Anschluss and die Infrastruktur. Die Funktion ist eine IDS/IPS ähnliche, die von den Inline Appliance Herstellern fokussiert angeboten wird. Ein typischer Markt für Startups im NAC Markt.

4.4 Remediation

Was muss man nun beachten, wenn ein System in Quarantäne kommt? Die Last im Support sollte dadurch nicht ansteigen. D.h. es sind Automatismen notwendig, um eine automatische Beseitigung des Schadens durchzuführen. Bei gemanagten Desktops mit Agenten ist dies „relativ einfach“ mit der Verknüpfung eines Patchmanagement Systems möglich, auf das Zugriff auch in der Quarantäne besteht. Eine universelle Funktion ist die Umleitung auf eine sog. Remediation Webpage, wo der Anwender Hinweise zur Beseitigung finden kann und durch den Prozess geleitet wird.

Dem Thema Remediation wird in Zukunft noch mehr Bedeutung zukommen. Insbesondere auch die Möglichkeiten der Integration mit Patch- und Update-Services wie WSUS (Windows Server Update Service) werden die Effektivität der Betriebs von NAC Lösungen erhöhen.

5. NAC Lösungen von Enterasys

Enterasys hat durch seine Secure Network™ Architektur eine Basis für switch basierte NAC Lösungen geschaffen. Für eine pre connect Assessment NAC Lösung sind neben den Switches selbst die Netsight® Komponenten Console, Policy Manager und Trusted Access Manager zusammen mit dem Trusted Access Gateway notwendig. Wobei die Wahl eines Assessment Servers (Netzwerkscan, Light Agent, Fat Agent) noch erforderlich ist. Enterasys unterstützt hier heute schon eine Reihe von Technologien und ist auch Mitglied der TCG. MS NAP Interoperabilität wurde ebenfalls schon demonstriert.

Eine post connect Assessment NAC Lösung erfordert noch die Netsight® Automated Security Manager Komponente sowie den Einsatz von Dragon® Intrusion Defense oder andere Intrusion Detection Technologien.

Weiterhin ist eine inline Appliance NAC Lösung durch den Einsatz der Matrix N Serie im Distribution Layer möglich. Diese Appliance kann auch das Trusted Access Gateway und in Zukunft die Dragon Funktion in einer einzigen Lösung beinhalten und vereint damit pre connect und post connect Assessment.

Eine out of band Appliance Lösung stellt die Enterasys Sentinel™ Lösung mit den Netsight® Komponenten Console und Trusted Access Manager zusammen mit dem Trusted Access Gateway dar. Hier können auch 3rd Party Geräte unterstützt werden, die 802.1X Authentisierung und VLAN Zuweisung mittels RFC3580 ermöglichen.

Damit ist Enterasys der einzige Hersteller, der mit einer Architektur alle möglichen hardwareorientierten NAC Lösungen abbilden kann.

6. Zusammenfassung

Der NAC Markt ist noch sehr volatil. Damit ist es schwierig für den Kunden, auf das richtige Pferd zu setzen. Generell ist darauf zu achten, dass der Hersteller eine flexible Architektur besitzt mit offenen Schnittstellen, um sich den Marktgegebenheiten anpassen zu können. Die Entscheidung, NAC einzuführen ist nicht nur eine technologische sondern auch eine organisatorische.

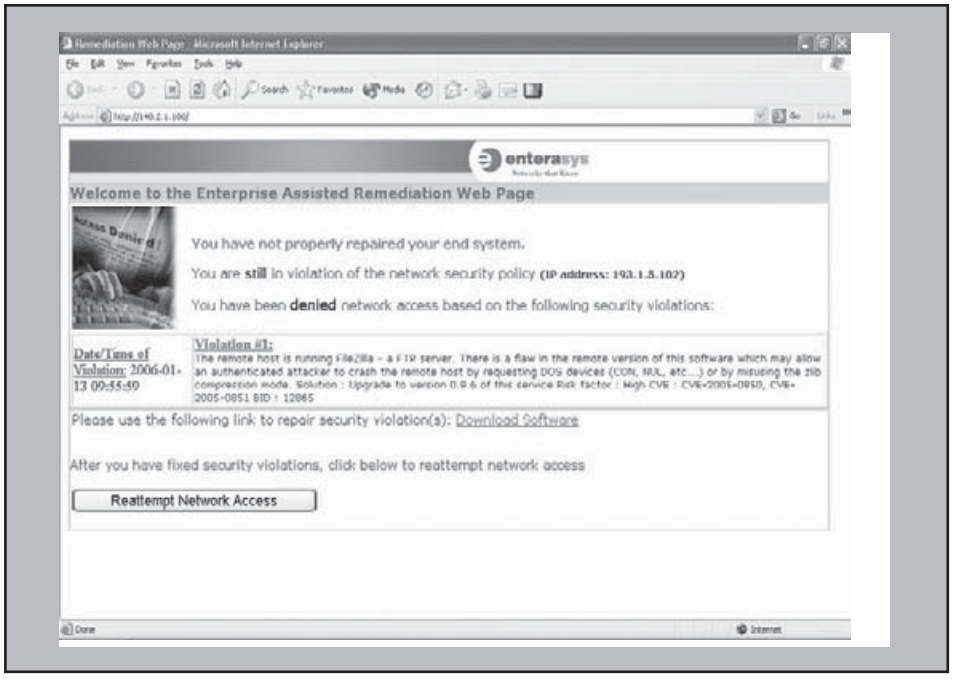


Abbildung 9:

Report des Monats

Quality of Service in modernen Infrastrukturen

Dieser Report bietet allen Betreibern von Netzen einen vollständigen Überblick über aktuelle QoS-Verfahren sowohl im LAN als auch in Wireless LANs und in WANs. Darüber hinaus werden alle Entscheider in die Lage versetzt, den Nutzen von Maßnahmen in QoS-Techniken abzuschätzen und mit alternativen Lösungen zu vergleichen. Sie erhalten aktuellste Informationen, die vor dem Hintergrund der zunehmenden Integration von VoIP-Telefonie und der verstärkten Konvergenz von Büro- und Produktionsnetzen bei keinem Netzwerkexperten fehlen darf.

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

Beispiel für eine Anwendung

Die höchsten QoS-Anforderungen in lokalen Netzen werden heutzutage durch Voice-over-IP-Technologien (VoIP) mit ihren sehr hohen Ansprüchen an geringe Verzögerungen und Varianzen bei der Zwischenankunftszeit von Paketen gestellt. Insbesondere die Paketlaufzeit stellt hohe Ansprüche an die subjektiv empfundene Qualität der Sprachübertragung. International wird hier von einem Grenzwert von 150 ms ausgegangen. Dabei muss aber berücksichtigt werden, dass diese Latenz nicht nur durch den Transport innerhalb des Netzes entsteht, sondern auch Rechenzeit für die Kodierung und Dekodierung an den jeweiligen Endstellen erforderlich ist.

Bei der Festlegung von Obergrenzen für Paketlaufzeiten für die Sprachkommunikation werden die folgenden Annahmen getroffen (siehe Abbildung 1):

- Die Verzögerung durch Kodierung und Dekodierung beträgt jeweils 10 ms.
- Weist ein Netz eine sich auf den Voice-Decoder negativ auswirkende Varianz der Paketlaufzeiten aus, muss auf der Empfängerseite eine Zwischenspeicherung der Pakete erfolgen, damit der zeitliche Abstand zwischen zwei aufeinander folgenden Paketen den Anforderungen des Empfängers entspricht. Die empfangsseitige Zwischenspeicherung geht auf Kosten des Gesamtbudgets für die Paketlaufzeit und ist daher zusätzlich von den tolerierbaren 150 ms abzuziehen. Für den Ausgleich der Laufzeitschwankungen wird daher ein Puffer von 20 ms auf der Empfängerseite vorgesehen.

Der Transportweg darf somit im Worst Case maximal Delay-Werte von 110 ms aufweisen, um die Delay-Anforderungen der Sprachkommunikation zu erfüllen. Um diesen Wert zu erreichen, ist es unter Umständen erforderlich, VoIP-Pakete mithilfe von QoS beim Transport durch das Netz zu priorisieren. Das in der Abbildung 2 dargestellte Schema zeigt ein Beispiel für die Anwendung von QoS in einem Ethernet-Netz.

Im ersten dargestellten Modell ist ein anderes Endgerät (z. B. ein PC) über einen Mini-Switch in einem IP-Telefon an das Netz angeschlossen. In diesem Modell muss das IP-Telefon den VoIP-Verkehr gegenüber dem Datenverkehr intern priorisieren. Darüber hinaus können für die verschiedenen Klassen unterschiedliche COS-Werte vom IP Phone gesetzt werden (COS steht für Class Of Service; jeder COS-Wert entspricht in diesem Beispiel einem UP-Wert gemäß IEEE 802.1D). Dabei wird das ggf. vorhandene COS-Feld im Paket des angeschlossenen PCs überschrieben.

Im zweiten Modell, das den separaten Anschluss von IP-Telefonen und anderen Endgeräten vorsieht, sind zwei Fälle denkbar:

- Die Ports, welche dem Anschluss der IP-Telefone dienen, werden als trusted port definiert, d. h. der Access-Switch akzeptiert an diesen Ports das gesetzte COS-Feld und handelt danach (Zuordnung der VoIP-Pakete zur Priority Queue). Die anderen Ports werden als untrusted konfiguriert, d. h. sämtlicher eingelesener Verkehr an diesen Ports wird der default queue zugeordnet. Die Anwendung dieses Modells setzt entweder eine Umkonfiguration der Switches bei Umzügen oder eine einheitliche Zuordnung voraus (Beispiel: Ports 1 bis 12 sind trusted und dienen dem Anschluss der Telefone, während die Ports 13 bis 24 untrusted sind und dem Anschluss anderer Endgeräte dienen).
- Alle Ports werden als trusted konfiguriert. Dieses Modell bedeutet, dass die von den PC-Anwendungen gesetzten Werte im COS-Feld vom Access-Switch unverändert akzeptiert werden und der Access-Switch danach handelt. Dies kann möglicherweise die Priorisierung des VoIP-Verkehrs gegenüber dem Datenverkehr aufheben, wenn bestimmte Anwendungen einen priorisierten COS-Wert setzen.

Bei der Priorisierung des Verkehrs im Netz stellt sich daher die grundsätzliche Frage, ob den Endgeräten vertraut wird oder die entsprechenden Felder explizit von den Netzkomponenten gesetzt werden. Im ersten Fall ist die Priorisierung des Voice-Verkehrs nicht sichergestellt. Im zweiten Fall sind Umzüge, Neuanschlüsse und Änderungen mit Umkonfigurationen verbunden, oder es müssen feste Port-Bereiche für verschiedene Endgerätetypen reserviert werden. In dem zweiten Fall ist die Priorisierung des Soft-Phone-Verkehrs nicht möglich.

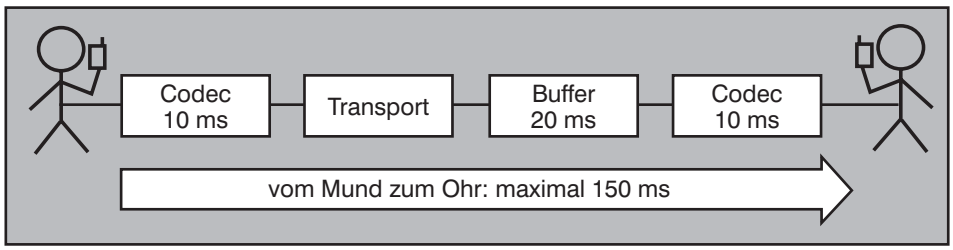


Abbildung 1: Delay-Annahmen

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

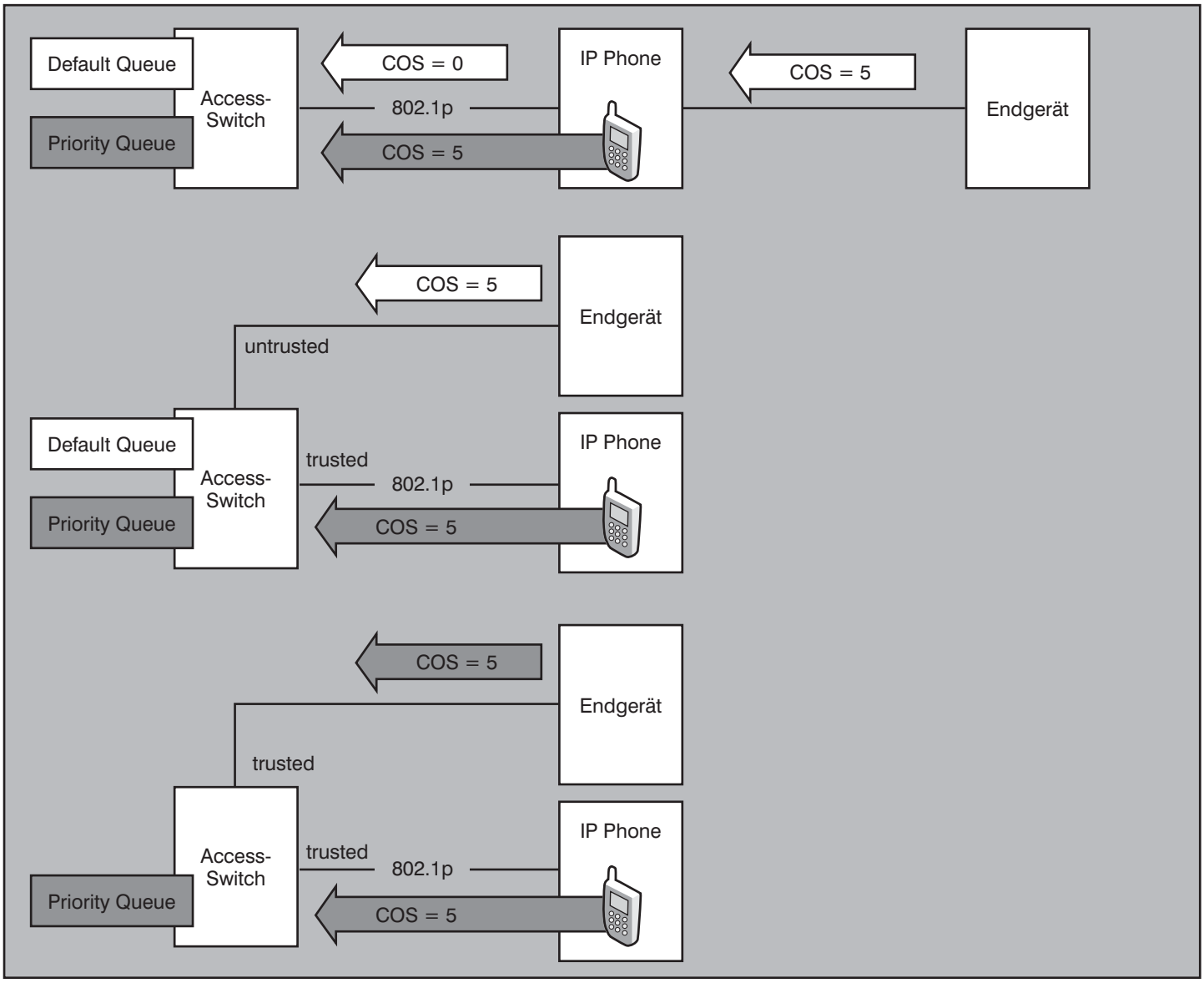


Abbildung 2: Priorisierung gemäß IEEE 802.1D/p

Schwerpunktthema

Die Wireless Maschen-Netz Revolution und UWEs

Fortsetzung von Seite 1

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

Nimmt man es genau, entsteht durch diese Konstruktion kein Funknetz, sondern die Möglichkeit des kabellosen Anschlusses von Endgeräten unter begrenzter Funkberegnung.

Aufgrund des Erfolgs von WLAN-Techniken haben die bestehenden Infrastrukturen zunehmend Schwierigkeiten, mit den vielen WLAN-Zellen angemessen umzugehen. Verbleiben wir bei den bisherigen Standards, gibt es grob drei Möglichkeiten:

- Das Distribution System ist ein großes, geswitchtes Ethernet. Dann kommt man sofort auf den Gedanken, die Switches mit Zusatzfunktionen auszurüsten, die die Schwächen der WLAN-Konstruktion ausbügeln. In Ermangelung eines Standards ist das sog. „WLAN-Switching“ oder „Controller-basiertes WLAN-Design“ bisher absolut proprietär, das heißt, man bleibt auf Gedeih und Verderb einem Hersteller ausgeliefert.

- Das Distribution System wird in Funktechnik nach IEEE 802.11 ausgeführt (nach aktueller Technik wäre das ein Wireless Distribution System WDS, das zum Beispiel die Auslegung des Distribution-Bereichs in 11a und den Endgeräteanschluss in 11g ermöglichen würde). Das ist zwar möglich, hat aber seine deutlichen Grenzen in Konstruktion und Performance. Immerhin wäre diese Lösung standardisiert und „Wireless“.

- Das Distribution System wird mit IEEE 802.16 WiMAX ausgeführt. Das ist technisch ausgesprochen elegant und hat viele Vorteile, die ich schon früher beschrieben habe. Nachteilig ist, dass wir es dann wieder mit einer neuen Funktechnik zu tun bekommen, die ihre eigenen Gesetze hat und ihrerseits wieder eigene Infrastrukturen benötigt und zum anderen das Problem letztlich nur „nach oben“ verschoben wird.

Alle diese Alternativen haben gemein, dass sie auf folgende strukturelle Probleme nur schlecht, mit hohem Aufwand oder gar nicht reagieren können:

- Ausfall von Access Points
- Ausfall des Funkmediums in dem Sinne, dass die zur Verfügung stehenden Kanäle kurzzeitig schwer gestört sind
- Dynamische Änderungen in der Anzahl von Stationen und Access Points bzw. in den genutzten Anwendungen
- Wechselnde Einsatzbedingungen
- Portabilität, also z.B. der Umzug eines ganzen Unternehmensteils woanders hin
- Dynamische Änderungen hinsichtlich der geforderten aggregierten Gesamtleistung oder relevanter Teile von ihr, einschließlich Änderungen der gewünschten Dienstqualität
- Dynamische Änderungen bei den Anwendungen

Wir werden auf diese Punkte nochmals gesondert eingehen, denn schließlich suchen wir eine Struktur, die mit all diesem wesentlich besser umzugehen vermag.

Schließlich stellt sich aber eine Frage massiv:

Wie kann ich auch in Zukunft eine große Anzahl quasistationärer und mobiler Endgeräte in ein möglichst flächendeckendes Funknetz flexibel, wirtschaftlich und leistungsfähig einbinden?

Die Antwort liegt eigentlich auf der Hand:
Durch die Verlagerung von Infrastruktur-Funktionen in die Endgeräte !

Und das ist der eigentliche Segen der Technologie der Maschennetze. Wie wir sehen werden, ermöglichen sie, dass sich die Endgeräte weitgehend selbstständig zu einem Netz organisieren, welches mit der Anzahl der Teilnehmer wächst und leistungsfähiger wird. Der Übergang vom selbst organisierenden Funknetz zu anderen, bestehenden Kabelnetzwerken wird durch neue, flexiblere Schnittstellen gewährleistet.

1.2 Grundsätzliche Vorzüge von Maschen-Netzen

Ohne sich auf eine bestimmte Technologie festzulegen, kann man die Vorzüge von drahtlosen Maschen-Netzen recht schnell erkennen.

Maschen-Netze, die in der Literatur auch oft als Multi-Hop-Netze bezeichnet werden, sind eine flexible Architektur für das effiziente Hin- und Herbewegen von Daten zwischen Geräten. In einem traditionellen WLAN müssen sich Stationen mit einem AP verbinden und die Kommunikation wird von diesem gesteuert und ggf. weitergeleitet. In einem Maschen-Netz kommunizieren die Knoten direkt oder indirekt untereinander, wobei ein Maschen-Knoten auch die Funktionen eines Access Points und/oder eines Ports haben kann, wie dies im Zusammenhang mit IEEE 802.11s ja bereits erläutert wurde. In einem Multi-Hop-Netz kann jede Station mit einer Radioverbindung als Router und/oder AP mit ggf. zusätzlichen Portfunktionen fungieren. Dabei ist ein zentraler Routing Algorithmus mit einer pfiffigen Metrik der Schlüssel zum Erfolg. Aber in diese Metrik kann man nicht nur Bewertungen hinsichtlich der Qualität von Wegen einarbeiten, sondern auch andere Parameter, wie z.B. die Belastung von z.B. APs oder Ports. Ist der „nächstgelegene“ AP oder Port zu sehr beschäftigt, kann es günstiger sein,

Die Wireless Maschen-Netz Revolution und UWEs

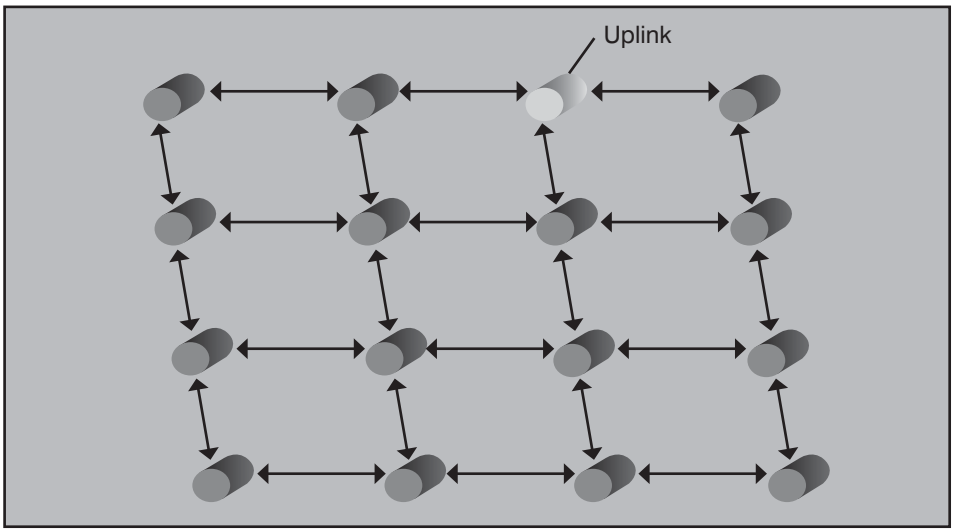


Abbildung 1: Maschen-Netz

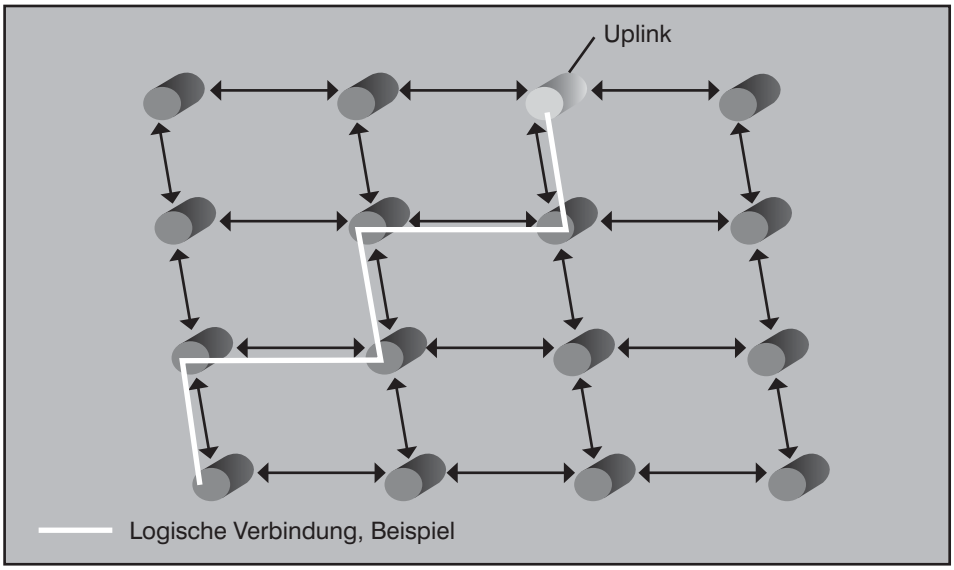


Abbildung 2: Maschen-Netz, Robustheit (1)

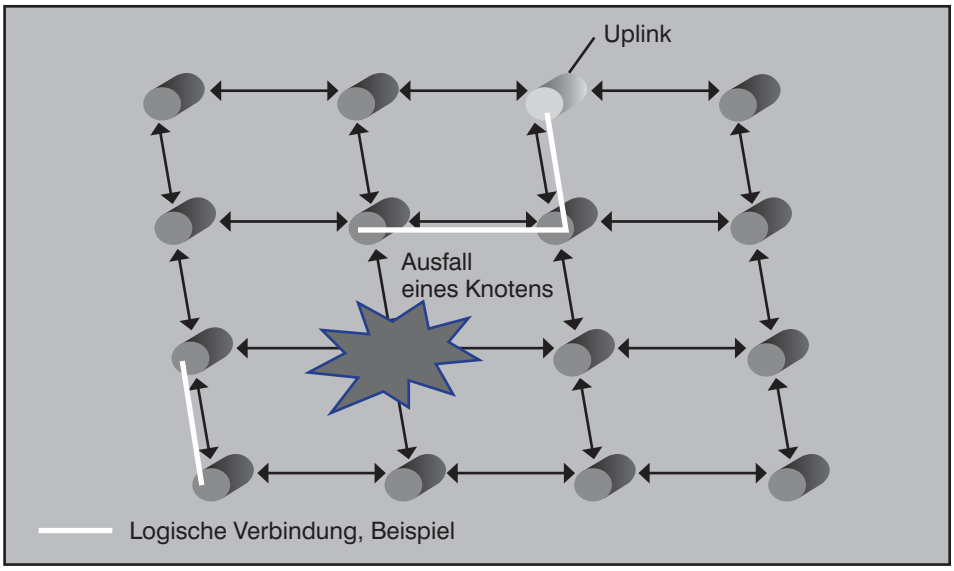


Abbildung 3: Maschen-Netz, Robustheit (2)

einen AP oder Port zu benutzen, der zwar weiter weg, aber geringer ausgelastet ist. Hier bieten sich wahre Spielwiesen zur Optimierung. (siehe Abbildung 1)

Maschen-Netze haben unabhängig von der Technologie, in der sie ausgeführt werden, folgende grundsätzliche Vorzüge gegenüber zentralisierten Strukturen:

- **Robustheit.** Ein Maschen-Netz ist wesentlich robuster als sein zentralisierter Kollege, weil es nicht in seiner Gesamtheit abhängig von der Leistungsfähigkeit einer singulären technologischen Komponente ist (bzw. deren einfach-redundanten Auslegung). Diese Robustheit wird durch die Möglichkeit der parallelen Nutzung unterschiedlicher Routen zwischen den Maschenknoten noch erhöht. Dies könnte man natürlich auch Anwendungs-spezifisch gestalten und auch Datenströme einzelner Anwendungen auf verschiedene Routen aufteilen. Natürlich wird man bestimmte Anwendungen von diesen Verfahren ausnehmen müssen (zum Beispiel Voice). (siehe Abbildung 2-5)

- **Höhere Bandbreite.** Die Physik des bei drahtloser Kommunikation eingesetzten Übertragungsmediums Luft diskutiert, dass die nutzbare Bandbreite bezogen auf eine Übertragungstechnologie und eine festgelegte Sendeleistung und den entsprechenden Antennengewinn umso höher ist, desto kürzer die Entfernung ist, die überwunden werden muss. Interferenzen und andere Dämpfungsfaktoren sorgen sozusagen dafür, dass umso mehr Daten verloren gehen, je größer die Distanz ist. Man kann dem mit schlauen Antennen und ausgefeilten Codierungstechniken sowie Signalsynthetisierung wie bei OFDM zwar in einem gewissen Maße gegensteuern, aber am Ende schlägt die grundsätzliche Physik immer durch. Ein Maschen-Netz ist demgegenüber umso leistungsfähiger, je enger die Maschen gezogen werden. Durch den Multi-Hop-Ansatz können dann größere Entfernungen leicht überwunden werden, eben mit ausreichend vielen kleinen Zwischenstationen. Gerade dem Problem der Kapazitätsbegrenzung in lizenzfreien Bändern kann damit begegnet werden. (siehe Abbildung 6)

- **Parallelverarbeitung.** In der Literatur wird hier auch von „Spatial Reuse“ gesprochen. Wenn zu viele Stationen Zugriff zu einem AP möchten, kann es zur Verstopfung kommen und aufgrund des wunderbaren DCF-Verfahrens geht

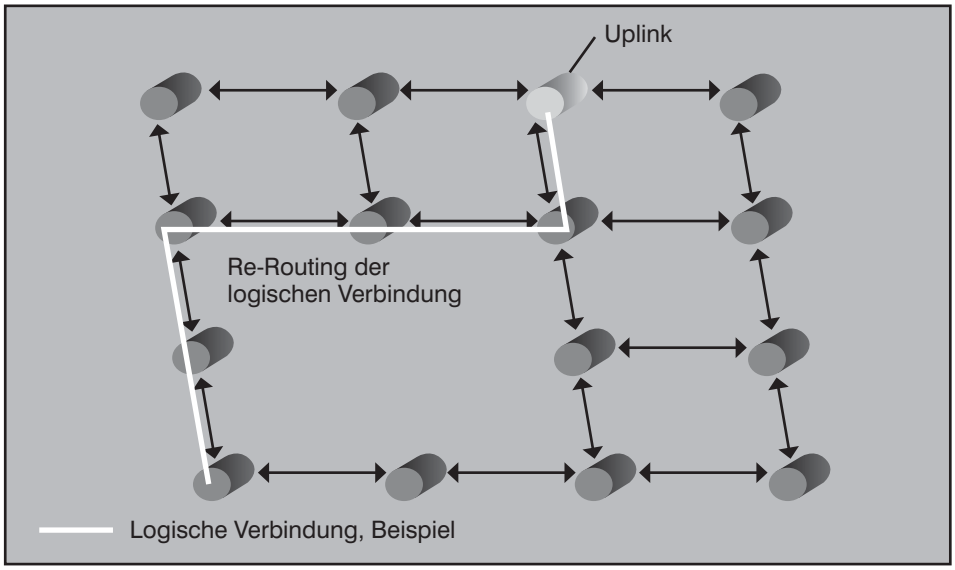


Abbildung 4: Maschen-Netz, Robustheit (3)

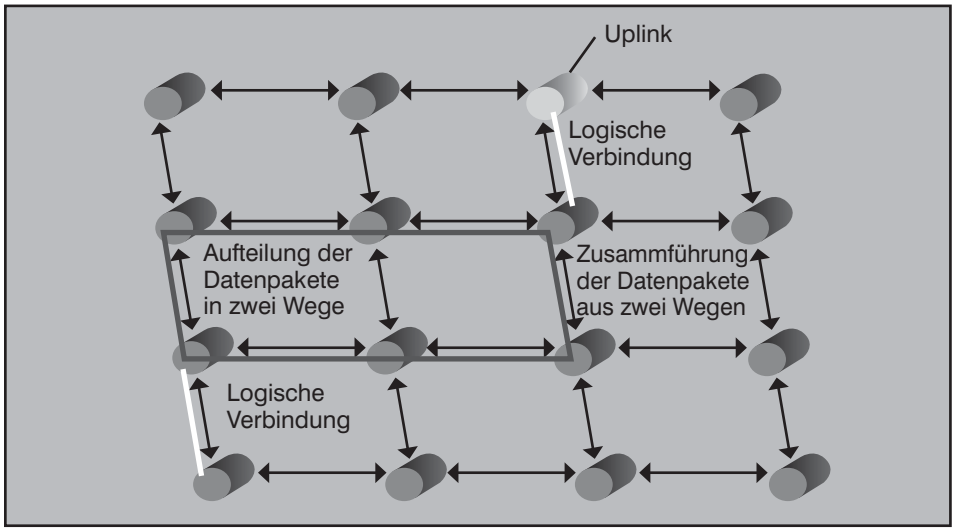


Abbildung 5: Maschen-Netz, Verteilung der Wege

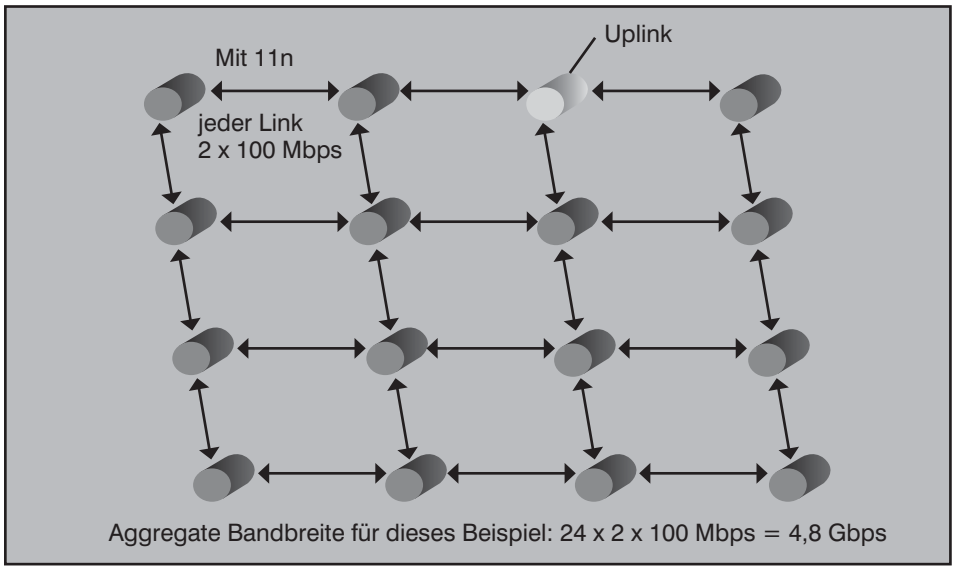


Abbildung 6: Maschen-Netz, aggregate Bandbreite

die Leistung schließlich in die Knie. Bei einem Maschen-Netz können viele Verbindungen gleichzeitig benutzt werden, ohne sich notwendigerweise gegenseitig zu stören. Auch das klappt natürlich umso besser, desto mehr Endgeräte auch eigenständige Maschen-Funktionalität haben. (siehe Abbildung 7)

Ein anderer Aspekt ist schließlich auch die sinnvolle Mehrfachverwendung von Frequenzbändern. Maschen-Knoten kommunizieren mit ihren Nachbarn. Bei IEEE 802.11s benutzen sie ein Band für die Steuerung der Kommunikation und springen für die eigentliche Datenübertragung auf ein anderes Band, natürlich unter Berücksichtigung von DFS und TPC. Das führt aber dazu, dass ein Band für die Datenübertragung nur „rund um einen Maschen-Knoten“ herum belegt ist, falls Rundstrahler als Antennen benutzt werden. Mit Richtstrahlern kann man das noch weiter optimieren. Wegen TPC kommt das Signal nur bis zu den direkten Nachbarn. Jenseits dieser Nachbarn, also sagen wir zur Sicherheit 2 Hops weiter kann die gleiche Frequenz wieder für die Datenübertragung benutzt werden, ohne dass man Störungen befürchten müsste.

1.3 Maschen-Netze und die Lösung der grundsätzlichen Problembereiche

Wir hatten ja weiter oben eine Reihe grundsätzlicher Problembereiche aufgezählt, die sich bei konventionellen WLANs ergeben. Diese Aufzählung ist sicherlich nicht vollständig. Wir wollen jetzt sehen, ob und wie Maschen-Netze hier zu günstigeren Ergebnissen kommen können.

- **Ausfall von Access Points.** In einem ersten Ansatz werden Maschen-Netze vielfach so aufgebaut sein, dass die Stationen keine eigenen Maschen-Fähigkeiten haben. Sie müssen also von Maschen-Knoten versorgt werden, die auch AP-Fähigkeiten haben. Fällt ein solcher Knoten aus, stehen sie natürlich genauso dumm da wie bei einem herkömmlichen WLAN. Mit der Zeit werden aber immer mehr Endgeräte Maschen-Funktionalität bekommen. Warum, sehen wir weiter unten im Artikel. In einem solchen Fall kommunizieren sie mit der Hilfe irgendeines Nachbarn. Fällt der aus, nimmt man eben einen anderen. Erst dann, wenn es keinen anderen Knoten mehr gibt, mit dem man kommunizieren könnte, fällt man in eine Isolation. Das Maschen-Netz arbeitet also umso besser, je enger es geknüpft ist.

- **Hinzufügen einer größeren Menge von Stationen** und Access Points mit

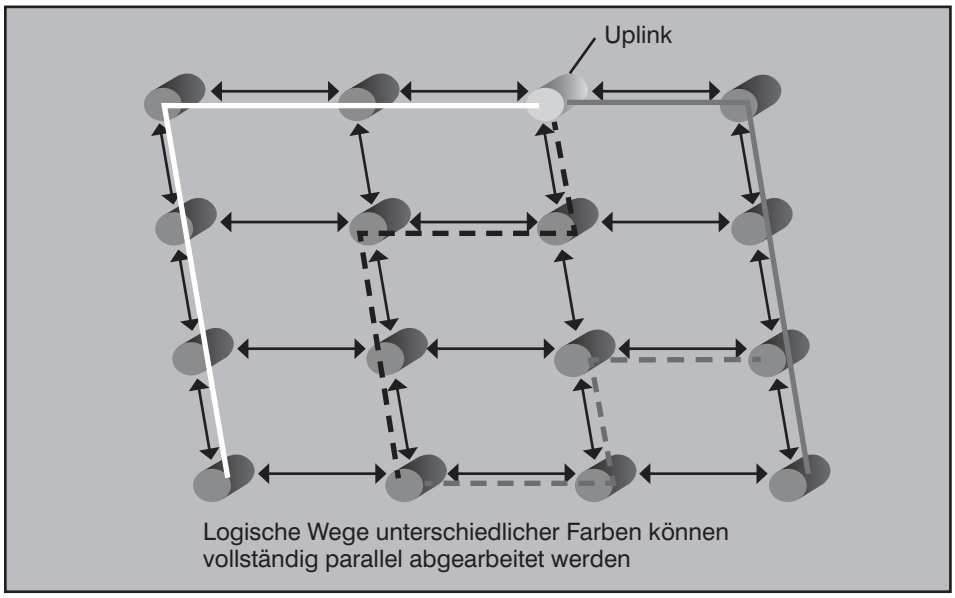


Abbildung 7: Maschen-Netz, Parallelverarbeitung

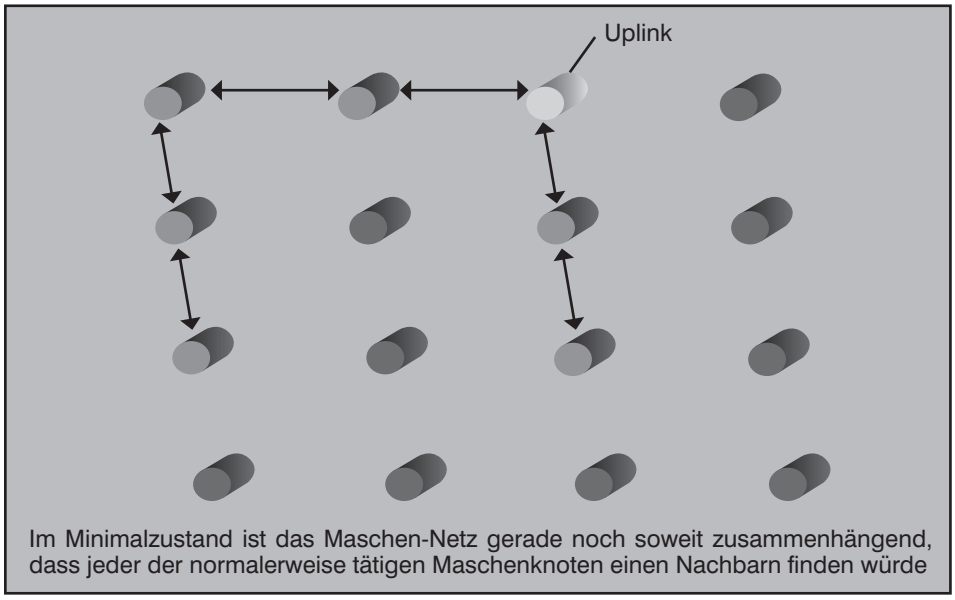


Abbildung 8: Party-System (1) Minimalzustand

wirklicher Dynamik. Mit herkömmlicher WLAN-Technik müssen hinzukommende APs einzeln installiert und an das DS angeschlossen werden. Also muss man konkret planen, wie viele Stationen sich in einem zu überdeckenden Gebiet schlimmstenfalls ansammeln könnten. Wegen der begrenzten Leistung einzelner Zellen wird man dann ggf. völlig unnötigerweise APs installieren, um z.B. in einer Hot Spot Lösung für den schlimmsten Andrang gerüstet zu sein. Besteht grundsätzlich ein Maschen-Netz, können im Grunde genommen beliebig viele Knoten zu beliebigen Zeitpunkten hinzutreten und das Maschen-Netz engmaschiger gestalten. Der charmante Nebeneffekt hierbei ist, dass sich die aggregierte Gesamtleistung des Netzes mit jedem hinzutretenden Knoten erhöht. (siehe Abbildungen 8-10)

- **Wechselnde Einsatzbedingungen.** Es kann sein, dass sich die Einsatzbedingungen für ein Netzwerk drastisch ändern. Hauptsächlich geschieht das durch die Einbringung neuer Dienste, die z.B. zu höheren Anforderungen an die Gesamtleistung oder an die Verzögerung führen. Statische hierarchische Netze können dabei schnell an Grenzen stoßen, die ein vollständiges Redesign oder einen Technologiewechsel erfordern. Bei Maschen-Netzen kann man die aggregierte Gesamtleistung durch die Hinzufügung neuer Maschen-Knoten erheblich und dynamisch steigern.

- **Dynamische Bewegungen** hinsichtlich der geforderten aggregierten **Gesamtleistung** oder relevanter Teile von ihr, einschließlich Änderungen der gewünschten Dienstqualität. Das hatten wir ja schon aus einer anderen Perspektive. Ein Maschen-Netz bemüht sich hinsichtlich der Dienstqualität immer darum, den schnellsten möglichen Weg bereitzustellen. Hier wird man auf Dauer mit dem, was in IEEE 802.11s momentan definiert ist, nicht auskommen. Es könnte z.B. nötig oder sinnvoll sein, den Maschen-Knoten die Möglichkeit zu spendieren, ankommende Pakete nach Prioritätsklassen in Warteschlangen zu sortieren, wie das ja auch schon früher für WLANs vorgeschlagen wurde. Dann kann jeder Maschenknoten dafür sorgen, dass Pakete, die einer höheren Prioritätsklasse angehören, bevorzugt geforwardet werden. Man muss hier das Rad nicht neu erfinden, sondern lediglich bewährte Mechanismen aus der Welt der Router auf die Maschen-Knoten übertragen. Die Möglichkeit dazu steckt heute im Konzept der Maschen-Netze schon drin, wird aber in einer ersten Stufe der Realisierung wohl noch nicht zu finden sein, aber man kann ja nie wissen.

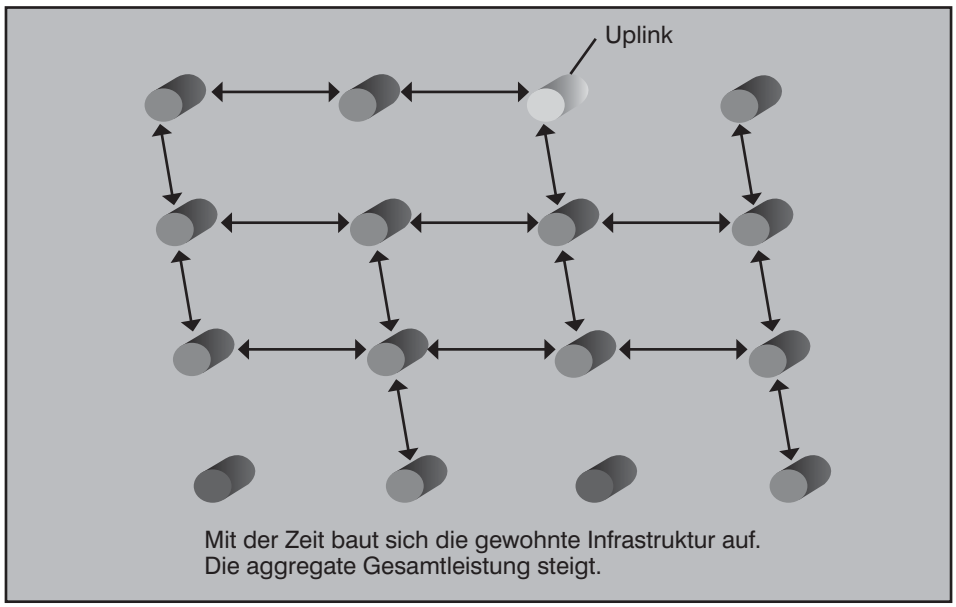
Soweit zu den Vorzügen der Maschen-Netze als strukturelles Konzept. Nun kommen wir dazu, wie die Knoten denn aussehen werden und welche Entwicklungen hier in absehbarer Zeit stattfinden werden.

2. Universal Wireless Entities UWE

Heute gibt es drei verschiedene Ansätze zur Gestaltung von Maschen-Netzen:

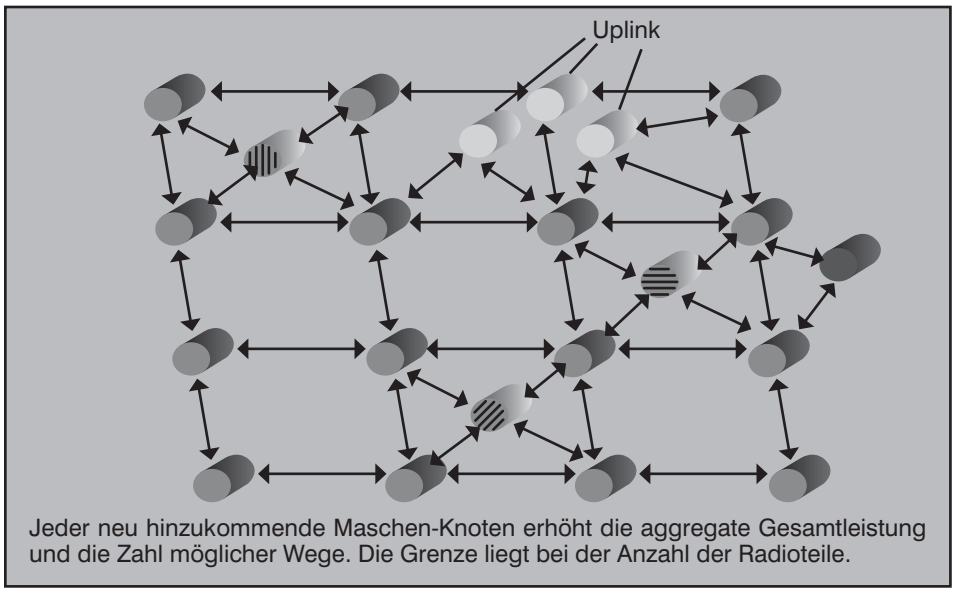
- Herstellerspezifische Maschen-Netze, die vor allem in Ermangelung eines Standards entstanden sind und heute schon an vielen Orten gute Dienste leisten. Beispiele hierfür sind Systeme der Hersteller Belair Networks, FireTide Networks, Strix, Tropos, Motorola, NetxtHop, D-Link, Intel usf. und auch die im Handel befindlichen Systeme von Cisco

- Maschen-Netze nach IEEE 802.11s, die dann auf den Markt kommen, wenn der Standard fertig ist, das wird Ende 2007/Anfang 2008 sein. Unterstützung für den Standard kommt vor allem von den etablierten Herstellern wie Cisco, Intel, Motorola, Nortel, Thomson sowie anderen. Haupt-Anwendungsbereiche sind Hot Spots, Unternehmens- und Industrienetze



Mit der Zeit baut sich die gewohnte Infrastruktur auf.
Die aggregate Gesamtleistung steigt.

Abbildung 9: Party-System (2) Infrastruktur



Jeder neu hinzukommende Maschen-Knoten erhöht die aggregate Gesamtleistung und die Zahl möglicher Wege. Die Grenze liegt bei der Anzahl der Radioteile.

Abbildung 10: Party-System (3)

- Maschen-Netze nach IEEE 802.16a WiMAX/HuMAN und zur Unterstützung von IEEE 802.16e Mobile WiMAX. Hier sind vor allem die Provider am Zug, weil die Frequenzbereiche von Regulierungsbehörden verteilt werden. Hauptanwendungsgebiete sind hier erwartungsgemäß Last Mile-Versorgung, Flächenabdeckung für Mobile WiMAX und die Versorgung weiterer öffentlicher Bereiche

Wir können eigentlich wie immer von Folgendem ausgehen:

- Proprietäre Systeme werden sich dauerhaft nicht durchsetzen können
- WiFi-orientierte Systeme werden sich am schnellsten und mit der höchsten Stückzahl durchsetzen, alleine wegen der Anwendung im Konsumer-Bereich
- WiMAX-Systeme werden sich soweit durchsetzen, wie echter, rechenbarer Bedarf für sie besteht.

Allerdings ist es unter diesen Bedingungen so, dass sich die Maschen-Netze hinsichtlich der eigentlich in ihnen ruhenden Möglichkeiten im Rahmen von IEEE 802.11s nicht vollständig entfalten können, weil wir hier ja immer noch die Struktur haben, dass die Maschen-Knoten an sich primär als Access Points für Stationen ohne Maschen Fähigkeiten benutzt werden, was schließlich die nutzbare Performance senkt und viele andere Vorzüge relativiert.

Aber: es ist eine Lösung in Sicht: Universal Wireless Entities.

2.1 Universal Wireless Entities

Eine Universal Wireless Entity ist ein Gerät, welches mehrere Radioteile für die Nutzung unterschiedlicher Funkdienste besitzt.

Wie wir intuitiv wissen und später noch genauer sehen werden, ist die aggregierte Gesamtleistung eines Maschennetzes davon abhängig, wie viele Radioteile die in ihm befindlichen Knoten haben und wie viele Verbindungen zu Nachbarn sie demgemäß gleichzeitig laufen lassen können.

Ganz mager ist ein einziges Radioteil, weil ja schon bei IEEE 802.11s mindestens zwei verschiedene Kanäle bedient werden müssen, nämlich der gemeinsame Synchronisationskanal und der Kanal, über den man aktuell mit einem Nachbarn Daten austauscht. Wegen der Vielzahl der Synchronisations- Routing und Verwaltungsnachrichten ist eine abwechselnde Bedienung dieser Kanäle mit nur einem Radioteil, welches laufend die Frequenz wechselt, zwar möglich, aber nicht besonders förderlich.

Es sollten schon zwei oder mehr Radioteile für einen Maschen-Knoten sein. Wenn das aber nun so ist, dann könnte man auch auf den Gedanken kommen, gleich Radioteile für unterschiedliche Funkdienste einzubauen. Das hört sich zunächst einmal sehr verwegen an, ist es aber, wie wir gleich sehen werden, überhaupt nicht. Der bisherige Gang der Standardisierung hat es nämlich mit sich gebracht, dass alle relevanten Standards mit Ausnahme des WiMAX für Festverbindungen die gleiche Sende- und Empfangstechnik verwenden, nämlich OFDM. Der Unterschied liegt i.W. nur in der unterschiedlichen Vorverarbeitung und Codierung der Signale, also außerhalb des eigentlichen Teils des Transmitters, der sich mit dem physikalischen Sende- und Empfangsbetrieb befasst. Wie eng die Verwandtschaft heute ist, sieht man auch, wenn man sich die Standards IEEE 802.11n für schnelle WiFi-WLANs und IEEE 802.16e für Mobile WiMAX genau ansieht: der wesentliche Teil mit den intelligenten Antennen ist in hohem Maße identisch. Kleinere Abweichungen ergeben sich aus den unterschiedlichen Entwicklungshintergründen.

Ein Universal Wireless Entity könnte z.B. Radioteile für folgende Dienste haben:

- IEEE 802.11 a,g,n
- IEEE 802.16 a,e
- GSM

Mit dem GSM-Teil kann ein UWE auch unter ungünstigen Bedingungen Verbindung mit einem anderen UWE eingehen. Das wäre z.B. praktisch für die Anbindung kleinerer Umgebungen, die so ungünstig liegen, dass sich eine andere Art der Anbindung nicht lohnt, denn GSM gibt es ja nun wirklich fast überall. Ein anderer Einsatzfall wäre z.B. dann gegeben, wenn die übliche Versorgungsform ausfällt, entweder weil das Medium gestört ist oder weil die Nachbarn, zu denen man üblicherweise Verbindung hat, kurzzeitig oder dauerhaft gestorben sind.

Mit dem Konzept der universellen Funkteile ergibt sich auch die wunderbare Möglichkeit, Maschen-Netze hochzuziehen und unterschiedliche Technologien zu integrieren. So könnte z.B. eine Reihe kleinerer Maschen-Netze zunächst nach WiFi arbeiten. Eröffnet dann ein Provider einen WiMAX-Service der für die Knoten funktechnisch erreichbar ist, können sie diesen auch sofort nutzen.

Dem aufmerksamen Betrachter stellt sich natürlich sofort die Frage, wie das denn eigentlich im Detail funktionieren soll. Auf die technische Basis kommen wir im nächsten Abschnitt. Logisch gesehen ist es lediglich erforderlich, die in einem Maschen-Netz vorhandene Metrik (die Basis für den Routing Algorithmus zwischen den Maschen-Knoten) so abzuändern, dass sie auch die Verwendung unterschiedlicher Funkdienste berücksichtigen kann. So könnte man z.B. eine WiFi-Verbindung als besonders „billig“ und eine GSM-Verbindung als besonders „teuer“ charakterisieren. Die Metrik, die in IEEE 802.11s vorhanden ist und die ich in meinem betreffenden Artikel besprochen habe, ist z.B. für eine solche Erweiterung hervorragend geeignet.

Eine UWE kann in einem Endgerät positioniert sein und für dieses Endgerät hervorragende Dienste leisten, weil es das Endgerät vernetzen kann, wenn es überhaupt irgendeine Art Funkdienst in der Nähe gibt.

Gleichermaßen kann man UWEs als strukturelle Einheiten benutzen, die zwar nicht direkt ein Endgerät bedienen, aber in gewissem Maße Löcher im Maschen-Netz stopfen. Wir müssen uns immer wieder vor Augen halten, dass IEEE 802.11s und IEEE 802.16a mit begrenzten Sendeleistungen in lizenzfreien Bändern arbeiten müssen und von daher die Reichweite natürlich begrenzt ist.

Eine weitere Ausführungsform wäre der UWE-AP, eine UWE, die gleichzeitig klassische Access Point Funktionen ausüben kann und damit Stationen versorgt, die noch keine eigene Maschen-Netz Funktionalität haben.

Ganz wichtig ist schließlich der UWE-Port, der eine Verbindung zwischen einem Maschen-Netz und anderen Netzen herstellen kann, wie das im Zusammenhang mit der Port-Funktion bei IEEE 802.11s ja schon hinreichend genau beschrieben wurde.

Wie zeitnah sind diese Überlegungen? Um diese Frage zu beantworten, muss man zu den Chipherstellern schauen, was wir im Folgenden tun werden.

2.2 UWE ante portas

Manchmal sind es einzelne Forschungsartikel, die die Basis für großflächige Revolutionen legen. Meist entstehen diese an Stellen, wo man sie nicht direkt sucht. So auch der Artikel mit dem harmlosen Titel „A 1,4 V, 2,4/5GHz CMOS System in a Package Transceiver for Next Generation WLAN“, der von Mitarbeitern der Fa. Intel auf dem Internationalen Symposium on VLSI Technology, welches jährlich abwechselnd von der IEEE und der Japanischen Gesellschaft für angewandte Physik durchgeführt wird, vorgestellt wurde. Inhalt des Artikels ist Folgendes.

Intel hat einen Prototyp für einen direktkonvertierenden Dual-Band Radio Transceiver vorgestellt, der in der Lage ist, jeden bestehenden WiFi-Standard zu unterstützen (also IEEE 802.11 a,b, und g) und darüber hinaus auch die funktionalen Ziele von 802.11n. Der Transceiver ist komplett in CMOS-Technik (Complementary Metal Oxide Semiconductor) ausgeführt und Bestandteil der sog. „System-in-a-Package“ (SIP)-Technologie, die es ermöglicht, integrierte CMOS-Radios mit gegenüber bisherigen Möglichkeiten wesentlich erweiterten Fähigkeiten zu konstruieren. Im Artikel werden die einzelnen „Baugruppen“ vorgestellt, die es ermöglichen, flexible Multimode-Radios im seit Jahren bekannten und erfolgreichen Standard-CMOS-Prozess herzustellen. Laienhaft ausgedrückt stehen diese Baugruppen für bestimmte Funktionen (A/D-Wandler, QAM-Codierer, OFDM-Synthetisierer mit IFFT, Sender, Empfänger, Steuerteil für Smart Antennas ...), wie wir sie aus den in den Standards manchmal befindlichen Blockdiagrammen kennen. Die Baugruppen sind dabei allerdings keine fertigen Chips, sondern eher eine Art Schablonen. Diese Schablonen kann man dann mit einer geeigneten Entwurfsmethode zusammenbringen, so wie es das funktionale Design verlangt. Ergebnis dieses Prozesses ist dann eine aus diesen Baugruppen-Schablonen zusammengesetzte neue Schablone, die die gesamte Funktionalität umfasst und dann ihrerseits in den CMOS-Produktionsprozess einfließt. Damit kann man dann z.B. einen Chip bauen, der die gewünschten Funktionen hat, oder die Schablone wiederum als Gesamtbaustein in ein neues Design, z.B. für einen Netzwerkprozessor, einfließen lassen.

Um zu hören, was Intel damit vorhat, zitieren wir Krishnamurthy Soumyanatha, den Direktor des Intel Labors für Kommunikations-Schaltkreise: „Das System-in-a-Package-Designs benutzt mehr Niederspannungsschaltkreise als wir jemals in der Vergangenheit benutzt haben, was bedeutet, dass wir es integrieren und zu niedrigeren Kosten produzieren können, wobei es bei niedrigen Spannungen läuft und ein längeres Leben der Batterien ermöglicht. Die variable Bandbreite dieser Lösung erweitert die Möglichkeiten weit über die 20 oder 100 MHz, die wir heute haben und wir erwarten, Datenraten von mehr als 100 Mbit/s zu unterstützen, die es den Leuten erlauben werden, mehrere hochqualitative Video-Streams gleichzeitig zu genießen."

Heute benutzt jedes Gerät ein speziell entworfenes Radioteil für die Verbindung zu einem speziellen Netzwerk, z.B. ein 802.11 a Radioteil für ein WiFi-WLAN. Ein anderes Gerät könnte ein völlig anderes Radioteil benutzen, z.B. für ein WiMAX-WMAN. Für die nächsten (wenigen!) Jahre erwartet Intel, dass mobile Geräte mehrere unterschiedliche Radioteile besitzen, damit sie an unterschiedlichen drahtlosen Netzen teilnehmen können. Intel´s Forschung zielt nun darauf, dass ein Gerät intelligente Antennen und ein rekonfigurierbares universelles Radioteil in einem einzigen Chip enthält, was die Kosten, die Größe und den Stromverbrauch erheblich senkt. Das Ziel ist die Fähigkeit, dass jedes beliebige Gerät sich jederzeit mit jedem beliebigen Netz verbinden kann. Eine der wichtigsten Voraussetzungen dazu, ist die gesamte dafür notwendige Herstellungstechnologie vollständig in den CMOS-Prozess einzugliedern, in dem Intel ja auch alle anderen Mikroprozessoren und Computerchips herstellt. Nur das hält die Kosten wirklich niedrig und ist ein Garant dafür, auch schnell sehr hohe Stückzahlen herstellen zu können. Das in der Arbeit vorgestellte Design arbeitet mit 1,4 Volt und erzielt damit einen erheblich geringeren Stromverbrauch als alles, was bisher auf dem Markt ist.

Letztlich ist es nach Aussagen des Entwicklungsdirektors das Ziel von Intel, die Fähigkeiten zur drahtlosen Kommunikation in alle zukünftigen (Prozessor-) Chips einzubauen.

Der vorgestellte Prototyp integriert einen 5 GHz CMOS Leistungsverstärker, der die spektrale Reinheit und die Interferenzfreiheit, wie sie von der US-FCC gefordert wird, erreicht. Hier werden spezielle Planungsmechanismen eingesetzt, die die Eigenheiten der Wellenausbreitung bei bestimmten Frequenzen schon im inneren Chipdesign berücksichtigen. All dies führt zu einer besseren Leistung. Um diese Resultate zu erreichen, hat Intel ein neues Kalibrierungsschema entwickelt, welches die Herstellung großer Mengen vereinfacht. Die Trennung von Effekten, wie sie bei Sendern und Empfängern bei getrennter Produktion in der Vergangenheit aufgetreten sind, hat sich als problematisch erwiesen. Baut man Sender und Empfänger mit Anwendung des Kalibrierungsschemas gemeinsam, wird die Qualität des Produkts deutlich erhöht.

Nun, damit haben wir genau, was wir brauchen, nämlich ein universelles Radio. Für die Konstruktion von Maschen-Netz-Knoten muss es dann nur noch einen Schaltkreis geben, der die verschiedenen zusätzlichen Verfahren, also hauptsächlich für Routing und Forwarding, abarbeitet. Zur Not könnte man das bei einem Endgerät auch in den Prozessor verlagern, denn die aktuelle Generation der Core2-Duo-Prozessoren, die ab dem Weihnachtsgeschäft 2006 in viele neue PCs und Notebooks verbaut worden ist, hat dazu sicherlich die notwendigen Leistungsreserven. Eine andere Möglichkeit wäre die Verwendung der mittlerweile wesentlich weiterentwickelten Netzwerk-Koprozessoren. Hier könnte man z.B. ein standardisiertes Verfahren in Hard- und Firmware implementieren, wie man das ja z.B. für Verfahren aus dem Bereich der Datensicherheit und Verschlüsselung erfolgreich macht und die Verwendung weiterer, z.B. herstellerspezifischer optimierter Verfahren durch entsprechende Assembler-Programme hinzuladen. Schließlich wird es aber darauf hinaus laufen, dass sich die Standardverfahren soweit stabilisieren, dass sie ganz in Hardware ausgeführt werden können und dann einfach eine weitere Baugruppe im SIP-Design darstellen.

Sie sehen also, die UWEs stehen unmittelbar vor der Tür, hier wird sich 2007 und 2008 allerhand bewegen.

3. Anwendungsbereiche für Maschen-Netze

Maschen-Netze haben klare Vorteile gegenüber hierarchischen Single-Hop-Netzen, die umso mehr zum Tragen kommen, je mehr Endgeräte Maschen-Fähigkeiten haben und je weniger Endgeräte auf die Versorgung durch AP-Funktionen angewiesen sind. Hierauf werden wir weiter unten nochmals eingehen. Zunächst aber zu wichtigen Anwendungsbereichen.

- **Home Networks.** Ein wesentlicher Anwendungsbereich ist natürlich der Heimbereich. Die wesentliche Stärke eines Maschen-Netzes in dieser Umgebung ist die Fähigkeit zum Transport großer Datenmengen, wie sie z.B. für hochauflösendes Fernsehen benötigt werden. Das können natürlich Lösungen nach bisherigen WLAN-Standards wie 802.11n auch, aber Maschen-Netze haben eine viel größere Flexibilität. UWEs können in alle Geräte wie HDTVs, PCs, Spielekonsolen, Camcorder usf. integriert werden und wenn man ein neues Gerät kauft, fügt es sich sozusagen von selbst in das bestehende Netz ein. Außerdem gibt es auch kaum Probleme mehr bei der Versorgung von Wohnflächen über 100 qm, bei denen bisherige WLANs ja oft einen zweiten AP benötigen, der dann doch irgendwie mit dem ersten verkabelt oder über ein Wireless Distribution System WDS verbunden werden muss. Der mögliche und erfolgreiche Einsatz in diesem Bereich steigert natürlich die Stückzahl und senkt den Preis für die Komponenten.

- **Corporate Networks.** Im Gegensatz zu allen anderen bekannten Lösungen sind die Maschen-Netze in der Lage, Last zu balancieren und haben eine wesentlich höhere aggregierte Gesamtleistung als hierarchische Single-Hop-Netze, die sehr elegant auf die Menge der Benutzer verteilt werden kann. Wenn die Preise für UWEs dahin kommen, wo der Autor sie erwartet, nämlich je nach Ausstattung in die Nähe bisheriger Kosten für Stationshard- und Firmware, haben Maschen-Netze das Potential, neben ihren sonstigen Vorteilen auch noch wesentlich billiger zu sein als bisherige Lösungen. Wir haben ja schon weiter oben die Reaktionen auf unterschiedliche Anforderungen diskutiert, so dass wir das hier nicht weiter ausführen müssen.

- **Hot Spots.** Ein Maschen-Netz kann durch seine enorme Flexibilität den Anforderungen in HotSpot-Umgebungen wesentlich besser Rechnung tragen als Systeme konventioneller Bauart. Dies gilt insbesondere für Hotspots mit stark dynamischen Client-Anzahlen wie zum Beispiel im Bereich von Flughäfen und Hotels.

- **Spontane Netze.** Alle Systeme, die eine UWE besitzen, können sich spontan zu einem Netz zusammenfinden. Das ist besonders nützlich bei Konferenzen u.ä.

- **Breitbandverbindungen** zu Service Providern. Die bisher für Maschen-Net-

ze in Frage kommenden Standards arbeiten auf Frequenzen, für die keine Sichtlinie zwischen den Stationen erforderlich ist. Ein ISP könnte z.B. eine grundsätzliche MAN-Verteilung auf WiMAX aufbauen und dann die Leistung mit Maschen-Knoten weiterverteilen. Das ist insbesondere interessant für alle Fälle, bei denen die WiMAX-Sendeantenne den Benutzer nicht richtig erreichen kann, weil es irgendwelche Hindernisse gibt. Die geschickte Positionierung einer UWE schafft hier schnell Abhilfe.

- **Industrieanwendungen.** Maschen-Netze schaffen interessante Lösungsmöglichkeiten für industrielle Anwendungen. Intel selbst erprobt z.B. zurzeit verschiedene industrielle Anwendungen einschließlich der präventiven Wartung in Halbleiterwerken. In den Intel Fabriken sind tausende Sensoren montiert, die Vibrationen, die von irgendwelchen Einrichtungen ausgehen, aufzuzeichnen, um ggf. absehen zu können, ob die Einrichtung demnächst defekt wird. Heute müssen die von den Sensoren aufgezeichneten Daten mühsam zusammengetragen werden, im Extremfall von Hand. Das ist lästig, teuer und uneffektiv. Außerdem führt das dazu, dass die Daten über den Zustand der Maschinen nur unregelmäßig basierend auf einer Annahme, wann die Maschine aufgrund ihres Alters und ihrer Belastung defekt werden könnte, gesammelt werden können. Eine Vernetzung der Sensoren wäre hier wirklich ein großer Vorteil, weil die Kosten erheblich gesenkt und die Vorhersagewahrscheinlichkeit für einen Ausfall wesentlich verbessert werden könnte. Eine Verkabelung ist in diesem Fall aber unpraktisch und leider ist es auch so, dass die Sensoren derart ungünstig verteilt sind, dass eine Lösung mit herkömmlicher WLAN-Technik auch unpraktisch ist, weil man bezogen auf die Anzahl der Sensoren sehr viele APs bräuchte. Ein Maschen-Netz ist hier die passendste Lösung. Dies ist nur ein Beispiel von vielen Möglichkeiten. Vor allem die hohe Ausfalltoleranz und die enorme Flexibilität von Maschen-Netzen sowie die Möglichkeit, die Komponenten weitestgehend von gefährlichen Umgebungen fernzuhalten oder sie nach entsprechenden Schutzklassen auszustatten, schafft hier wichtige Perspektiven. Von den Überlegungen zu Wireless Lösungen im industriellen Umfeld weiß man, dass es nur wenige Umgebungen gibt, die so beschaffen sind, dass der Funkverkehr wegen vielfältiger Störungen nicht sinnvoll möglich ist. In diesen Fällen können Maschen-Netze natürlich auch nichts ausrichten.

- **Mobile Anwendungen.** Mit der Entwicklung der IEEE 802.16e Mobile WiMAX-Netze sehe ich die klare Tendenz, dass Betreiber den Maschen-Netzen einen gewissen Vorzug gegenüber hierarchischen Netzen geben möchten. Der Grund dafür liegt auf der Hand: Kostenoptimierung. Für die Einführung eines Dienstes benötigt man nur eine gewisse Flächendeckung und damit sozusagen eine minimale Anzahl von Versorgungspunkten. Wird der Service von den Kunden gut angenommen, stehen Leistungserweiterungen unmittelbar an. Diese sind bei Maschen-Netzen aber besonders einfach durch Hinzufügung von mehr Maschen-Knoten und einer Verdichtung des Netzes zu realisieren. Das können hierarchische Strukturen auch bei WiMAX nicht so einfach in diesem Maße. Der Grund dafür ist, dass auch für einen öffentlichen Carrier die Funkbänder von der Regulierung her beschränkt sind, meist hat er diese Bänder ja gekauft. Startet der Provider einen Service mit festen Masten, haben diese eine meist ausreichende Abdeckung und können sofort die Leistung bringen, die das Band erlaubt. Die Leistung kann danach aber nicht mehr beliebig durch Hinzufügen neuer Maste gesteigert werden und eine Verbreiterung des Bandes ist auch nicht so ohne weiteres möglich. Im Grunde genommen bieten die Maschen-Netze hier durch die Verdichtung ohne Erweiterung des notwendigen Frequenzbandes Möglichkeiten, die es sonst nicht gibt. Eine Analogie wäre bei den optischen Ringen in DWDM-Technik zu sehen: auch hier konnte ein Betreiber mit einer vergleichsweise geringen Anfangsinvestition starten und die Kapazität nach dem Bedarf der Subscriber langsam aber sicher ausbauen. Das hat natürlich technisch überhaupt nichts mit den Maschen-Netzen zu tun, aber das zugrunde liegende Geschäftsmodell ist nahezu identisch und war im optischen Bereich sehr erfolgreich.

4. Einige Bemerkungen zur Leistungsanalyse von Maschen-Netzen

Eine allgemeine Leistungsanalyse von Maschennetzen ist relativ komplex, vor allem, weil es eine Reihe von Parametern gibt, die erheblichen Einfluss auf ein Analyseergebnis haben und teilweise recht schwer zu modellieren sind. Um nicht den Rahmen dieses Artikels zu sprengen, möchte ich hier nur einige Bemerkungen machen und mich darauf beschränken, einen ganz wesentlichen Punkt näher herauszuarbeiten.

Generell ist es so, dass ein Maschennetz eine erhebliche theoretische aggregierte Gesamtleistung hat. Diese ist im homogenen Fall, also bei identischer Ausführung aller Maschenknoten das Produkt aus der Anzahl der Maschenknoten, der Anzahl der Radioteile in jedem Maschenknoten und der Übertragungsleistung jedes dieser Radioteile. Ein Maschennetz bestehe

z.B. aus 100 Knoten mit je drei Radioteilen nach IEEE 802.11a. Dann wäre die aggregierte Gesamtleistung ca. 15600 Mbit/s. oder ca. 15 Gbit/s. Im inhomogenen Fall, also bei verschiedener Ausstattung der Geräte und verschiedener Leistung der Radioteile ergibt sich ein entsprechender Summenterm.

Leider steht uns die aggregierte Gesamtleistung je nach Ausführung des Systems nicht vollständig für die Datenübertragung zur Verfügung. Ein Maschennetz nach IEEE 802.11s ist so organisiert, dass ein Kanal immer für die Systemkontrolle, das Routing usf. benutzt wird. Also ist ein Radioteil schon mal damit beschäftigt, wenn wir annehmen, dass ein Radioteil nicht wechselweise am Kontrollkanal teilnimmt und Daten überträgt. In diesem Fall würde sich für das o.g. Beispiel die aggregierte Datenrate auf 10 Gbit/s. reduzieren.

Das ist natürlich im Vergleich mit bisherigen WLAN-Konzepten eine ganze Menge. Wie viel davon in der Praxis tatsächlich ausgenutzt werden kann, hängt von weiteren Parametern, z.B. der mittleren Weglänge, der maximal erreichbaren Kapazität usf. ab. Das ist aber an und für sich gesehen alles nichts Neues, denn der einzige wesentliche Unterschied zwischen den hier betrachteten Netzen und allgemeinen Multi-Hop-Netzen besteht ja im Übertragungsmedium.

Man kann also keinesfalls davon ausgehen, die aggregierte Datenrate immer vollständig ausnutzen zu können.

Andere Ergebnisse einer Leistungsanalyse betreffen Dinge wie mittlere und maximale Verzögerungszeit, die letztlich für die Gewährleistung von QoS wichtig sind. Hier spielt vor allem die Leistung des verwendeten Routing-Verfahrens eine wichtige Rolle. Diesem ist es aber sehr gleichgültig, ob es auf Geräten arbeitet, die mittels Drähten oder Glasfasern untereinander verbunden sind, oder ob die Geräte sich gegenseitig anfunken. Also können wir auch hier auf die Leistungsanalysen zurückgreifen, die für die bekannten Routing-Verfahren gemacht worden und die Grundlage jeder Router-Konstruktion sind. Letztlich kommt es darauf an, wie die Prozessoren für die Abarbeitung des Routing-Verfahrens ausgestattet sind und wie schnell sie arbeiten. Im Falle von IEEE 802.11s erwarte ich keine zusätzlichen Probleme durch den Kontrollkanal, weil dieser zwar mit DCF verwaltet wird, aber, wenn keine anderen Nachrichten auf ihm verarbeitet werden müssen, wegen der wenigen beteiligten Stationen und der geringen Nachrichtenlängen einigermaßen deterministisch arbeiten sollte. Probleme kann es dann geben, wenn die Hersteller die Systeme einfach zu sparsam ausstatten und diese an der Berechnung von Routen zu lange rechnen müssen. Andererseits erwarte ich bei den herkömmlichen Anwendungen einen Effekt, den man schon lange bei verdrahteten Multi-Hop-Netzen beobachtet: wenn das Netz einmal in Betrieb ist, ist der Anteil der neu auszurechnenden Routen relativ gering, es sei denn, es geschehen Veränderungen (Hinzufügen oder Wegfall von Maschenknoten, schwere Fehler, usf.) am Netz. Das war ja auch immer eine der Hauptbegründungen für die Verwendung von Source Routing: hat eine Station einmal den Weg zu einer anderen Station gefunden, mit der sie kommunizieren möchte, wird sie diesen auch eine gewisse Zeit benutzen.

Bei den in den nächsten paar Jahren zu erwartenden Systemen nach IEEE 802.11s und IEEE 802.16a wird die Routing-Problematik keinen wirklich wesentlichen Einfluss auf das Gesamt-Leistungsverhalten haben. Es ist daher momentan noch nicht an der Zeit, über weitere Alternativen nachzudenken. Ein Bedarf für schwerwiegendere Änderungen wird dann entstehen, wenn die Maschen-Netze wirklich sehr groß werden, also mit vier- oder fünfstelliger Anzahl von Knoten. Dann wird man sicher über mehrstufige komplexere Routing-Verfahren nachdenken müssen. Aber im Gegensatz zu meiner sonstigen Haltung bin ich sicher, dass die Hersteller, die das betrifft, schnell genug ihren bisherigen Erfahrungsschatz nutzen werden, um zu sinnfälligen Lösungen zu kommen. Das betrifft sinngemäß auch andere Bereiche wie Ende-zu-Ende Flusskontrolle usf.

Ich möchte hier statt einer weiteren allgemeinen Diskussion lieber den Platz nutzen, um ein sehr nahe liegendes Thema zu isolieren, nämlich die Verwendung von Stationen ohne Maschenfähigkeit in einem Netz, welches mit Maschen-Knoten ausgestattet ist, die AP-Funktionen nach altem Muster haben.

Dazu erweitern wir die Perspektive jetzt auf ein allgemeines Distribution System, so, wie wir es von 802.11 kennen. Das DS verbindet unterschiedliche WLAN-Zellen und das DS kann z.B. sein:

- ein Ethernet-Segment
- ein Funk-DS, welches ein Ethernet-Segment nachmacht
- ein Maschen-Netz mit Maschen-Knoten, die AP-Funktionalität haben
- ein Ethernet-Switch
- ein sog. „Wireless Switch“, also ein mit speziellen Controller Funktionen angereicherter Ethernet-Switch

Was ich jetzt wissen möchte, ist, ob es aus performancetheoretischer Sicht überhaupt einen wirklichen Unterschied macht, was wir als Distribution System verwenden, und zwar für den Fall, dass eine Station in einer WLAN-Zelle via AP, DS und fremdem AP mit einer anderen Station in einer anderen Zelle kommuniziert. Das ist die zentrale Frage, wenn es um symmetrische Anwendungsprofile geht, wie ich sie weiter oben beschrieben habe. (siehe Abbildung 11)

Eine größere Infrastruktur besteht für die Zwecke der Analyse aus einer Menge von (hoffentlich weitestgehend) überlagerungsfreien WLAN-Zellen, die mit einer DS-Struktur untereinander verbunden werden. (siehe Abbildung 12)

Wir machen jetzt folgende optimistische Voraussetzungen:

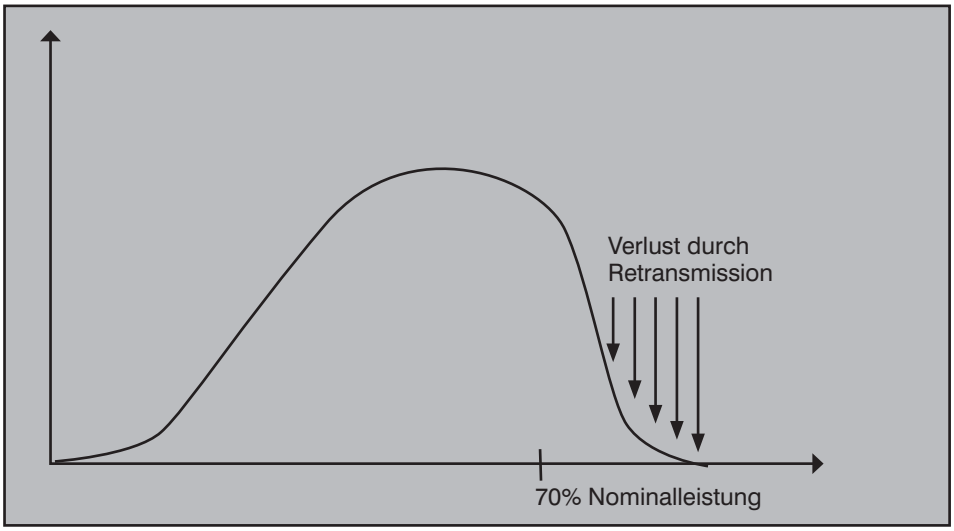


Abbildung 11: Erinnerung: Durchsatz von DCF (grob)

Die Wireless Maschen-Netz Revolution und UWEs

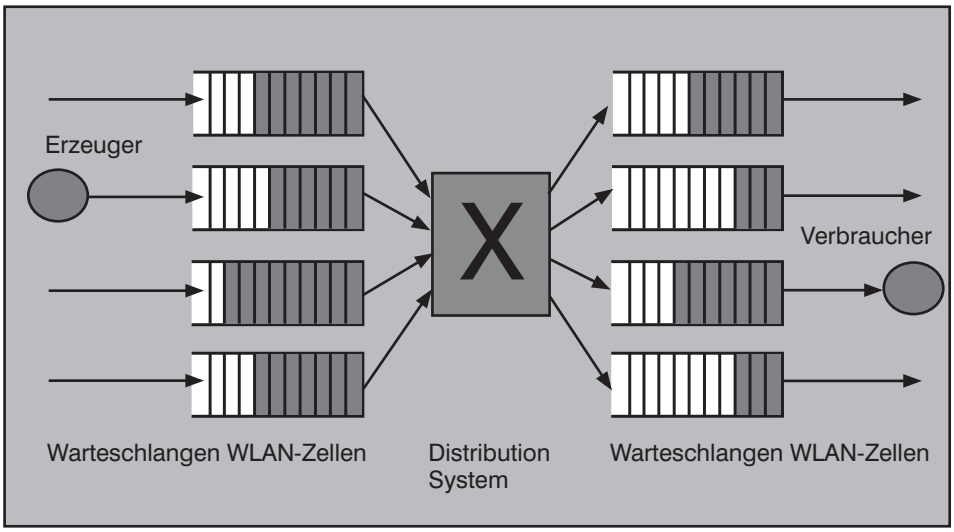


Abbildung 12: Modellierung der Infrastruktur

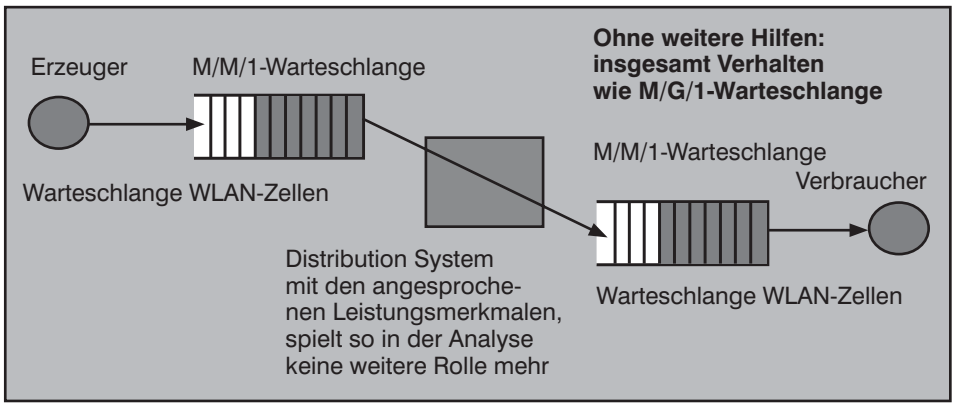


Abbildung 13: Reduktion des Analyseproblems auf Tandem

- die DS-Infrastruktur arbeitet mit gegenüber den WLAN-Zellen massiv überragender Leistung (stimmt für die meisten oben angegebenen Alternativen)
- die DS-Infrastruktur arbeitet daher mit einer zu vernachlässigenden Verzögerung (stimmt auch für Maschen-Netze, wenn der Routing-Algorithmus gut implementiert wurde)
- zwei durch die Switching-Infrastruktur verbundene WLAN-Zellen können so modelliert werden, als seien sie unmittelbar miteinander verbunden (folgt unmittelbar aus den bisherigen Annahmen)

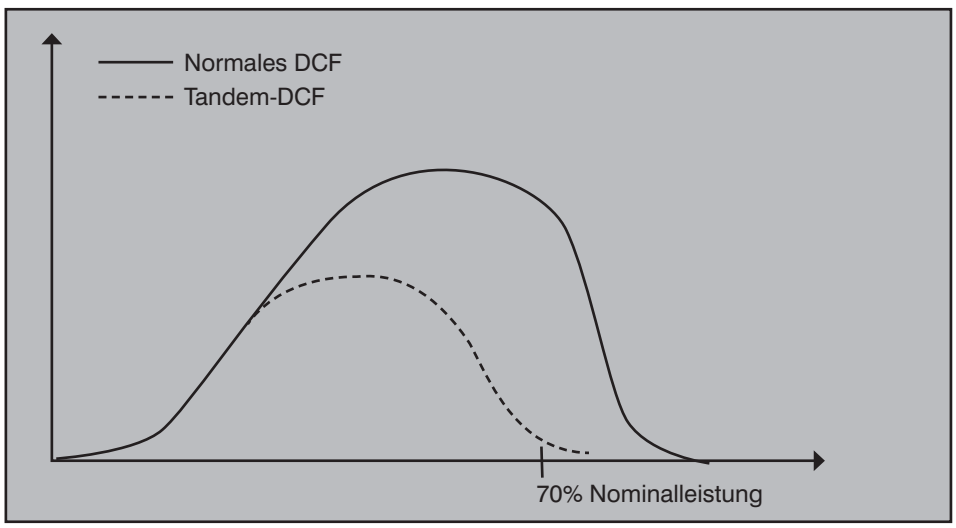


Abbildung 14: Durchsatz von DCF vs. Tandem-DCF

Dadurch entsteht ein sog. Offenes Queueing-Modell mit Tandem-Queues. (siehe Abbildung 13)

O.b.d.A. gilt dann zunächst die Kleinrock´sche Unabhängigkeitsannahme: die einzelnen WLAN-Zellen können einzeln modelliert werden. Dabei ergibt sich jedoch das Problem, dass die Länge einer bestimmten Nachricht, nachdem sie aus einer Exponentialverteilung gewählt wurde, fest ist. Das bedeutet, dass die Bedienzeiten an den zwei (oder mehr) Warteschlangen nicht unabhängig sind. So könnte die zweite (dritte, vierte, ...) Warteschlange nicht mehr unabhängig modelliert werden, weil ihr Eingangsstrom ja aus dem Ausgangsstrom der ersten Warteschlange besteht.

Da aber auch die Stationen in einer Zelle weiterhin nicht nur über die DS-Struktur, sondern auch untereinander kommunizieren, kann ohne wesentliche Verfälschung angenommen werden, dass sich einfach eine neue Mischung der Nachrichtenlängen ergibt.

Somit gilt Burke´s Theorem, dass die mittleren Verzögerungen einfach addiert werden können.

Wenn man weiter nichts unternimmt, haben zwei (oder mehr) hintereinander geschaltete M/M/1-Warteschlangen die asymptotische Leistung einer einzelnen M/G/1-Warteschlange. Die mittlere Verzögerung und mittlere Warteschlangenlänge kann in diesem Fall über die Formeln von Pollaczek-Khinchine hergeleitet werden.

Dies bedeutet im Klartext, dass die „Hintereinanderschaltung“ von zwei (oder mehr) WLAN-Zellen dazu führt, dass vom so entstehenden Gesamtsystem höchstens die Hälfte der Leistung (mindestens das Doppelte der mittleren Verzögerungszeit) einer individuellen Zelle zu erwarten ist, wenn man es auf den Verkehr bezieht, der beide (oder mehr) Zellen durchqueren muss, weil Quelle und Ziel in verschiedenen Zellen liegen.

Bringt man dieses nun in den Kontext der Ergebnisse, die für die mittels DCF verwalteten einzelnen WLAN-Zellen bereits seit Jahren vorliegen, kommt man zu einer erschütternd schlechten Gesamtleistung von Ende zu Ende. (siehe Abbildung 14)

Der interessierte Leser mag das gerne nachrechnen, für die Distribution Systeme ergibt sich allerdings folgende unangenehme Konsequenz:

Solange das nicht-deterministische DCF

das primäre Verwaltungsverfahren für Stationen in WLAN-Zellen ist, ist die mittlere Ende-zu-Ende-Leistung über mehrere Zellen hinweg bei symmetrischen Anwendungen so schlecht, dass es im Grunde genommen ziemlich gleichgültig ist, welche Art Distribution System eingesetzt wird, es kann daran auch nicht wirklich etwas retten.

Ich möchte es noch mal anschaulich darstellen: werden z.B. zwei WLAN-Zellen nach IEEE 802.11n mit je 100 Mbit/s. Leistung mittels eines irgendwie gearteten Distribution Systems untereinander verbunden, sinkt die Ende-zu-Ende-Leistung unter den Wert, den man bekommen würde, wenn die zwei kommunizierenden Stationen in einer einzigen IEEE 802.11a-Zelle liegen. Das heißt, dass man bei symmetrischem Verkehr über mehrere WLAN-Zellen hinweg im Grunde genommen eine ganze Technologie-Entwicklungsstufe verliert!

Daraus können wir, um wieder etwas konstruktiver zu werden, Folgendes ableiten:

Die volle Performance eines Maschen-Netzes wird sich genau umgekehrt proportional zur relativen Anzahl von alten Stationen entwickeln, die noch mit AP-Funktionalität versorgt werden müssen und selbst keine Maschen-Funktionalität haben !!!!!

Das bedeutet im Klartext, dass wir nur von einigen Vorzügen des Maschen-Netzes, wie z.B. der Robustheit, profitieren können, wenn wir es als großes Distribution System für konventionelle WLAN-Zellen einsetzen.

Erst dann, wenn auch die überwiegende Anzahl der Endteilnehmer-Stationen selbst Maschen-Funktionalität besitzen, kommen alle Vorzüge von Maschen-Netzen wirklich zur Geltung.

5. Herausforderungen im Zusammenhang mit Maschen-Netzen

Es gibt, wie eigentlich für jede neuartige Technologie, eine Reihe von Herausforderungen für die Konzeption von Maschen-Netzen, die vor der weiträumigen Einführung beachtet werden müssen:

- Installation
- Kosten
- Interoperabilität
- Koexistenz mit anderen Netzen und Systemen
- Quality of Service
- Sicherheit

Die **Installation** ist eigentlich nur im Heimbereich eine Herausforderung. Die bestehenden Standards müssen um einige Prozeduren für das Plug & Play erweitert werden, was ja auch bereits von einer Reihe von Herstellern gemacht wird. Alles in allem wird es erst dann komplizierter, wenn unterschiedliche bestehende und neue Netze in größerem Maße zusammengeführt werden müssen. Hier sind besonders die Ports zwischen den Maschen-Netzen und den bestehenden Lösungen von Interesse.

Es ist schon heute so, dass für bestimmte Anwendungsfälle die Kosten für ein Maschen-Netz deutlich unter denen für ein altes hierarchisches Netz liegen, obwohl die Maschen-Knoten alle noch nicht in großer Stückzahl gefertigt werden und dementsprechend vergleichsweise für sich gesehen noch teuer sind. Mit der zunehmenden Verbreitung werden sich die Kosten eindeutig zu Gunsten von Maschen-Netzen verlagern. Das gilt besonders für den Fall von z.B. Providern, die mit einer geringen Anfangsinvestition starten und das Netz nach den Anforderungen der Subscriber erweitern können. Bei Corporate Netzen sind natürlich alle Endgeräte interessant, die Maschen-Funktionalität haben und somit in dem Moment, wo sie das Netz benutzen, auch dessen aggregierte Performance steigern.

Die **Interoperabilität** auf der IP-Schiene dürfte damit sicherzustellen sein. Mögliche Probleme gibt es mit den unterschiedlichen Generationen von Radioteilen, die ja durch die bisherige Ausbreitung von WLANs in Hülle und Fülle herumstehen.

Die **Koexistenz** mit anderen Netzen und Systemen hat mehrere Perspektiven. In einer IEEE 802.11 Umgebung sieht es so aus, dass man zwar Maschen-Netze mit Funkschnittstellen nach IEEE 802.11b oder g ausrüsten kann, dies ist aber nicht besonders sinnvoll, weil man höchstens drei Kanäle parallel betreiben kann und davon ja einer für die Synchronisation benutzt werden muss. Die Koexistenz mit anderen Funkdiensten oder bestehenden WiFi-Netzen im 2,4 GHz-Band ist zwar möglich, es kann jedoch zu erheblichen Performance Problemen kommen, die die ganze Sache völlig zunichte machen. Ein IEEE 802.11s-Maschen-Netz gehört ins 5 GHz-Band, weil es nur dort genügend Kanäle gibt und weil auch durch die Funktionen TPC und DFS eine Koexistenz mit anderen in diesem band befindlichen Netzen durchaus sinnvoll zu gewährleisten ist. Angesichts der vielen Vorzüge eines Maschen-Netzes wird man aber nicht unnötig lange Access Points nach altem hierarchischem Muster und Maschen-Knoten neben einander betreiben, sondern vielmehr die AP-Fähigkeiten in die Maschen-Knoten integrieren und von daher die Versorgung der älteren, nicht maschenfähigen Endgeräte sicherstellen. Ebenfalls denkbar wäre die Koexistenz von WiFi-und WiMAX-Maschen-Netzen im 5 GHz-Band.

QoS: ich hatte weiter oben schon erwähnt, dass es bei größeren Lösungen sicherlich sinnvoll ist, darüber nachzudenken, intelligente Mechanismen für die Lastverteilung im Maschen-Netz einzuführen, um die zunächst ja nur rein theoretisch zur Verfügung stehende aggregierte Bandbreite besser ausnutzen zu können. In bestehenden „verdrahteten“ Multi-Hop-Netzen bestehen solche Lösungen ja heute auch schon und man wird im Laufe der Zeit sehen, was man davon sinnvoll übernehmen kann. Das betrifft letztlich auch Lösungen für die Sicherstellung von QoS und weiter oben hatten wir ja schon die Einführung unterschiedlicher Verkehrsklassen diskutiert. Es ist sicher sinnvoll, sich hier aus dem zu bedienen, was die Standardisierung z.B. durch IEEE 802.11e vorgibt.

Ein weiterer Problembereich ist natürlich **Security.** In einem Gebäude werden unterschiedliche Wireless Systeme koexistieren und sich ggf. überlappen. Es ist aber kein Problemfall sichtbar, der sich nicht auch bei der Verwendung von WLANs mit herkömmlicher Technik ergeben würde. Generell ist die Versendung von Informationen durch die Luft riskant. Ebenfalls riskant ist es natürlich, dass die Informationen geforwardet werden und somit auf Zwischenkonten zumindest eine kurze Zeit anwesend sind. Das sind aber keine neuen Risiken gegenüber WLANs einerseits und verdrahteten Multi-Hop-Netzen andererseits, z.B. hinsichtlich der möglichen Positionierung von Angreifern usf., so dass es nicht notwendig ist, neue Methoden zum Schutz zu suchen, sondern vielmehr die systematische Anwendung bestehender und bewährter Methoden im Vordergrund stehen sollte.

6. Die Evolution der Maschen-Netze und Designfragen

In diesem Abschnitt möchte ich nach den ganzen Vorüberlegungen weiter konkretisieren, was man nun mit Maschen-Netzen ab heute tun kann.

6.1 Die Evolutionsstufen der Maschen-Netze

Ich hatte ja schon weiter oben angedeutet, dass die Maschen-Netze zwar jetzt schon einen gewissen Erfolg und für bestimmte Anwendungen auch einen hohen Reiz haben, aber das ist erst der Anfang der Entwicklung.

Evo-Stufe 0: (2006/2007) heute erhältliche, proprietäre Maschen-Netze, bei denen die Maschen-Punkte Access Point-Funktionalität haben und die Teilnehmer-Stationen mit einem der bekannten WiFi-Funkstandards versorgen. Das Maschen-Netz ist in diesem Falle ein reines Infrastruktur-Netz.

Obwohl es mit Ausnahme der Funkschnittstellen zu den Teilnehmern noch keine „verbauten" Standards gibt, haben die Maschen Netze der Evo Stufe 0 schon eine Reihe von Anwendungen gefunden:

- Versorgung öffentlicher Bereiche (Hot Spots) auch im Zusammenhang mit Metropolitan Area Networks, Flughäfen, Bahnhöfen, Häfen
- Last-Mile für den Zugang von Haushalten zu Providern
- Öffentliche Sicherheit, Videoüberwachung
- Medizinische Bereiche wie Notdienste, Krankenhäuser
- Industrielle Anwendungen wie weiter oben beschrieben
- Logistik-Anwendungen
- Industrie- und Medienparks
- Veranstaltungsbereiche, Stadien usf.

Überall dort scheint es praktisch zu sein, auf eine starre Vernetzung wie sie durch die alte WiFi-Struktur vorgegeben ist, zu verzichten und statt dessen entsprechende Maschen-Netze aufzubauen, die natürlich primär Stationen bedienen, die keine Maschen-Fähigkeit haben. Offensichtlich gibt es einen breit gestreuten Bedarf, von der sternförmigen WiFi-Struktur abzukommen und mehr Flexibilität zu erhalten, auch wenn von der eigentlichen Leistung her die Vorteile der Maschen-Netze wegen der mangelnden Maschen-Fähigkeit der Endgeräte noch nicht vollständig ausgeschöpft werden.

Evo-Stufe 1: (2007/2008) wie Evo-Stufe 0, aber mit einem Standard (IEEE 802.11s oder IEEE 802.16a oder e) auch zwischen den Maschen-Knoten.

Diese Stufe unterstützt natürlich die bereits bestehenden Anwendungsbereiche, öffnet aber gleichermaßen den Markt. Das ist immer der gleiche Effekt, wenn von proprietären zu standard-basierten Systemen übergegangen wird. Dadurch wird zum einen das Spektrum der Systeme größer, zum anderen sinken die Kosten für die Geräte deutlich wegen der höheren Stückzahlen. Auch wenn im Einzelfall ein Betreiber ein Maschen-Netz nach wie vor bei nur einem Hersteller kauft, hat er dennoch ein wesentlich besseres Gefühl als vorher. Außerdem werden bestimmte Hersteller ermutigt, Nischenprodukte anzubieten, die sie vorher mangels einer Standardisierung nicht realisieren konnten.

Die Ausbreitung der Systeme erfolgt hauptsächlich in den in einem früheren Abschnitt genannten Haupt-Anwendungsbereichen. Mit der Verbreitung wird wie üblich eine Konsolidierung mit anderen Standards, z.B. im Hinblick auf die Sicherheit, leistungsfähigere Funkschnittstellen usf. erfolgen. Bestimmte Hersteller werden der Versuchung nicht widerstehen können, ihre jahrzehntelangen Erfahrungen mit Multi-Hop-Netzen in die Verfahren für Routing, Forwarding und Flußkontrolle einfließen zu lassen. Ich bin sicher, dass wir dann auch über entsprechende Erweiterungen der Standards reden werden, denn das heutige Standard-Angebot ist wirklich nur ein Basis-Baukasten, mit dem sich aber jetzt schon viel anfangen lassen wird.

Die Systeme dieser Stufe leiden wahrscheinlich noch an schwachen Prozessoren in den Maschen-Knoten und es könnten Performance-Engpässe durch zu langsame Abarbeitung von Routing-Verfahren usf. entstehen. Die schnelle Verarbeitung derartiger Verfahren ist aber neben verschiedenen anderen Aspekten auch die Voraussetzung für die Gewährleistung von hinreichender Mobilität bei Teilnehmern. Hier werden die Mobile WiMAX-Systeme allerdings einen gewissen Vorsprung haben und es wird auf dieser Seite sicherlich noch eine Menge Entwicklungsarbeit geleistet werden.

Evo-Stufe 2 (2008/2009): wie Evo-Stufe 1, aber mit zunehmendem Einfluss der UWEs. Bis jetzt werden die Maschen-Netze schlicht an zuwenig Radioteilen leiden. Ich nehme an, dass die Ausstattung der Evo-Stufe 1 höchstens 2 oder 3 unabhängige Radioteile beinhaltet. Wenn die Maschen-Netze aber immer „engmaschiger" werden, machen auch mehr Radioteile einen Sinn. So werden sich die entsprechenden Hersteller nicht die Gelegenheit entgehen lassen, auf der Basis der jetzt schon patentierten neuen Herstellungsverfahren wirklich leistungsfähige Maschen-Knoten auf die Beine zu stellen, z.B. mit 4-8 Radioteilen und einem leistungsfähigen Coprozessor, der nicht nur verschiedene Verfahren für z.B. Routing umfasst, sondern auch im Hinblick auf die Weiterverarbeitung in TCP/IP-Stacks und z.B. Kryptographischen Verfahren Erhebliches leisten kann. Außerdem haben sich natürlich die Funkschnittstellen auf der Basis von IEEE 802.11n weiterentwickelt.

Evo-Stufe 3 (2009/2010): endlich wird auch der überwiegende Teil der Teilnehmer-Endgeräte hinreichende Maschen-Fähigkeiten aufweisen, um das weiter oben angesprochene „Party-Prinzip" angemessen zu unterstützen. Die UWEs kommen in die Endgeräte, z.B. mit einer neuen Centrino-Generation. Die Funkschnittstellen werden pro Endgerät mindestens 100 Mbit/s unterstützen und die Maschen-Netze werden in der Lage sein, diese Leistung mühelos weiterzuleiten. Damit können letztlich alle heute denkbaren mobilen und fixen symmetrischen und asymmetri-

schen Anwendungen sehr leistungsfähig unterstützt werden.

Wie immer kann es sein, dass die Abschätzung der Zeiträume gewisse Missweisungen aufweist. Das persönliche Gefühl des Autors ist es aber, dass sich vor dem Hintergrund der aktuellen Entwicklungen besonders bei den Prozessoren und der VLSI-Technik die oben genannten Intervalle eher zusammenschieben als strecken.

6.2 Designüberlegungen für Evo-Stufen 0 und 1

Es wurden im Verlaufe des Artikels ja schon sehr viele unterschiedliche Anwendungsbereiche angesprochen. Tatsache ist, dass die erste Ausbreitungswelle der Maschen-Netze schlicht genau da stattfindet, wo man mit herkömmlichen Strukturen nicht weiterkommt. Maschen-Netze können immer da sofort erfolgreich Fuß fassen, wo

- die physikalische Wellenausbreitung herkömmlichen Strukturen Grenzen setzt
- Versorgungslücken einigermaßen elegant und kostengünstig geschlossen werden müssen
- mit Benutzern „dünn“ besiedelte Bereiche erschlossen werden sollen
- die Dynamik der geforderten Anwendungs-Szenarien eine Planung im herkömmlichen Sinne unmöglich macht

In diesem Zusammenhang ist es auch klar, wie wichtig die Standardisierung für den Erfolg der Systeme ist.

Hinsichtlich der Leistung hat man Ansprüche an den Durchsatz und die maximale Verzögerung. Obwohl das Konzept der Maschen-Netze einen erheblichen möglichen aggregierten Gesamtdurchsatz und auch die Möglichkeit für QoS und geringe Verzögerung in sich trägt, kann hier auf der Produktseite sehr viel verdorben werden. Wenn die Prozessoren zu lange an den Routen herumrechnen, ist es mit einem guten Delay vorbei, wenn die Zwischenspeicher ungünstig ausgelegt sind, kann es ebenfalls zu Verzögerungen und Stockungen kommen und wenn die Maschen-Knoten zu wenige Radioteile haben, ist es auch schnell vorbei mit der möglichen großen Gesamtleistung und der Nutzung der weiteren Vorteile wie Selbstorganisation, Selbstheilung, Dynamik, Party-Prinzip und so fort. Das sind aber alles keine neuartigen Probleme, die gab es mit den Routern auch. Ich erwarte im Zusammenhang mit den Maschen-Netzen auch das Aufleben alter Diskussionen hinsichtlich verschiedener Funktionen der Layer 2 und 3. Tatsache ist, dass die meisten bekannten Routing-Verfahren (und angelagerte Verfahren für Forwarding, Flusskontrolle ...) davon ausgehen, dass die Leitungen immer sofort verfügbar sind. Das kann man beim Medium Luft und der Funkübertragung nicht immer so ohne weiteres annehmen und hier werden wir ggf. noch einige spannende Überraschungen erleben.

Hinsichtlich der Reichweiten kann man nicht erwarten, dass die Funkschnittstellen, wie sie in den einschlägigen Standards definiert sind, größere Weiten erzielen als in anderen Umgebungen. Also gelten letztlich die gleichen Überlegungen, wie wir sie schon für Access Points konventioneller Bauart durchgeführt haben. Änderungen ergeben sich lediglich dann, wenn die Maschen-Knoten z.B. untereinander mit höherer Leistung arbeiten könnten. Das ist für die regulationsfreien Bänder aber zunächst auszuschließen.

Nicht vergessen darf man die Leistungsanforderungen bei den Netzübergängen. Solange noch asymmetrische Anwendungen benutzt werden, und die werden wohl nie ganz aussterben, ist deren Wohl und Wehe von der Leistung der Maschen-Ports abhängig. Durch die Möglichkeit vieler parallel benutzbarer Wege in einem Maschen-Netz kommen da schnell vergleichsweise hohe Anforderungen zusammen, die selbst bei kleinen Maschen-Netzen schnell mehrere Hundert Megabit/s. betragen können. Natürlich bietet die Konstruktion der Maschen-Netze auch den wunderbaren Vorteil, beliebig viele Maschen-Ports einzuführen. Das ist nicht nur zweckmäßig für die Gewährleistung von Redundanz, sondern auch sinnvoll für die Abarbeitung einer größeren Gesamtlast. Allerdings werden in diesem Falle Verfahren zur Lastverteilung und für die Gewährleistung von QoS notwendig, aber die gibt es ja.

Dies führt letztlich zu einer Optimierung der Wege durch das Maschen-Netz.

In den Evo-Stufen 0 und 1 kann man davon ausgehen, dass die Teilnehmer-Stationen selbst keine Maschen-Fähigkeiten haben und deshalb praktisch alle Maschen-Knoten Access Point Fähigkeiten benötigen.

7. Konsequenzen für die Unternehmensnetze

Die Maschen-Netze stellen ein so attraktives Designkonzept dar, dass sie ihren Platz in der unternehmensweiten Datenverarbeitung, bei Providern, in privaten Haushalten und an noch vielen anderen Stellen finden werden. In einer ersten Welle werden sie bestehende Strukturen nicht ersetzen, sondern um eine wesentlich flexiblere Anbindungsmöglichkeit für Endgeräte ergänzen. Jeder verantwortliche Betreiber ist aufgefordert, sich angesichts der schnellen und vielfältigen Änderungen in den Anwendungen und Anwendungs-Profilen nach Strukturen umzusehen, die wirklich zukunftsfähig sind. Und das sind die Maschen-Netze, auch wenn sie, wie alles Größere, zunächst einmal klein anfangen.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Kommunikationssysteme, Kollaborationssysteme und Anwendungsintegration vor dem Hintergrund der Netz-Konvergenz, 26.02. - 27.02.07 in Bonn

In diesem 3-tägigen Seminar werden sowohl die Einflüsse der Konvergenzfelder und Technologien auf das Design der Unternehmensnetze diskutiert, als auch die Potentiale, die sich daraus ergeben.

Preis: € 1.390,- zzgl. MwSt.

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

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

Preis: € 1.690,- zzgl. MwSt.

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

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

Preis: € 2.290,- zzgl. MwSt.

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

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

Preis: € 1.390,- zzgl. MwSt.

Wireless LAN: Planung, Produktauswahl, Installation, Trouble Shooting, 05.03. - 09.03.07 Hilton in Bonn

Dieses 5-tägige Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. Die letzten beiden Tage sind optinonal buchbar und liefern vertiefte Kenntnisse zur Planung, Konfiguration und Betrieb von flächendeckenden sicheren WLAN und Hotspots, ergänzt durch praktische Beispiele und Demonstrationen.

Preis: € 2.290,- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 05.03. - 09.03.07 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.

IP-Telefonie Anwenderschulung: Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung in der Praxis, 05.03. - 06.03.07 in Bonn

Dieses 2-tägige Seminar beschreibt die Planung, Installation und den Betrieb einer IP-Telefonie-Komplettlösung auf Basis vernetzter Cisco CallManager ergänzt um Zusatzprodukte. In einem Unternehmensnetz wurden bereits 50 der über 100 Standorte mit Systemen und über 15.000 IP-Telefonen ausgestattet. Die im Zusammenhang mit einem VoIP-Projekt stehenden, wesentlichen Aspekte werden in einem Mix aus Erfahrungsberichten und technischen Beiträgen betrachtet.

Preis: € 1.390,- zzgl. MwSt.

Windows Vista - Tatsächlich Mehrwerte vorhanden?, 13.03.07 in Bonn

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

Preis: € 990,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 12.03. - 14.03.07 in Köln

Der Referent dieses 3-tägigen Seminars vermittelt seine jahrelange Projekt-Erfahrung bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld.

Preis: € 1.690,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 12.03. - 16.03.07 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.

CCNE

ComConsult Certified Network Engineer

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

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

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

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

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

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

CCTS

ComConsult Certified Trouble Shooter

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

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

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

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

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

CCSE

ComConsult Certified Security Expert

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

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

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

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

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

Impressum

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

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

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen