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

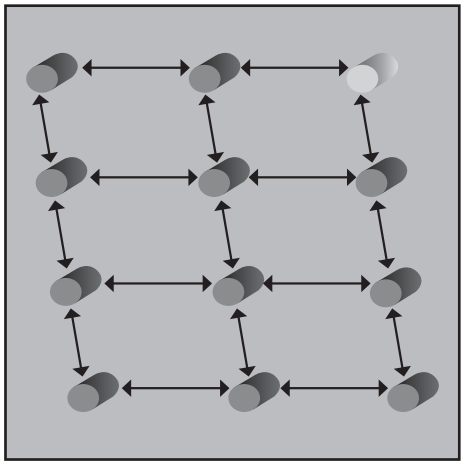
von Dr. Franz-Joachim Kauffels

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 Hersteller-abhängigkeit

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

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.

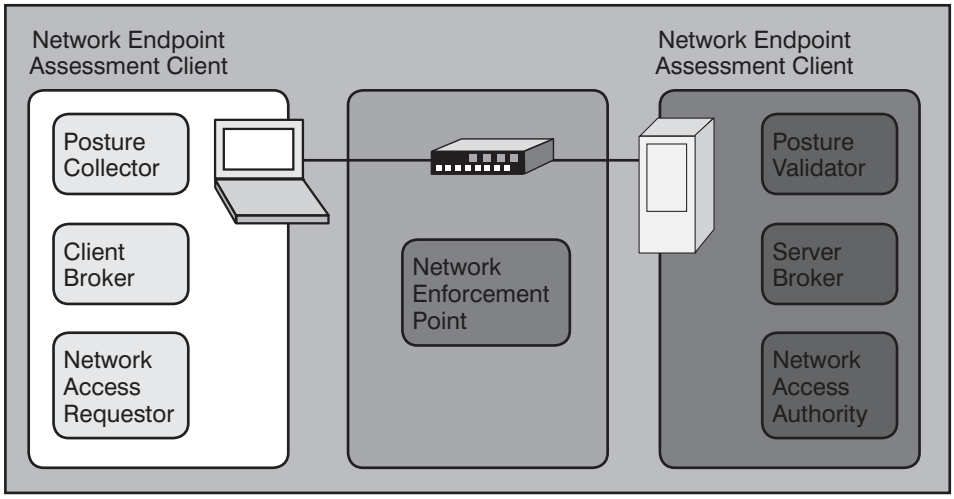


Abbildung 1: Funktionseinteilung der IETF

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)

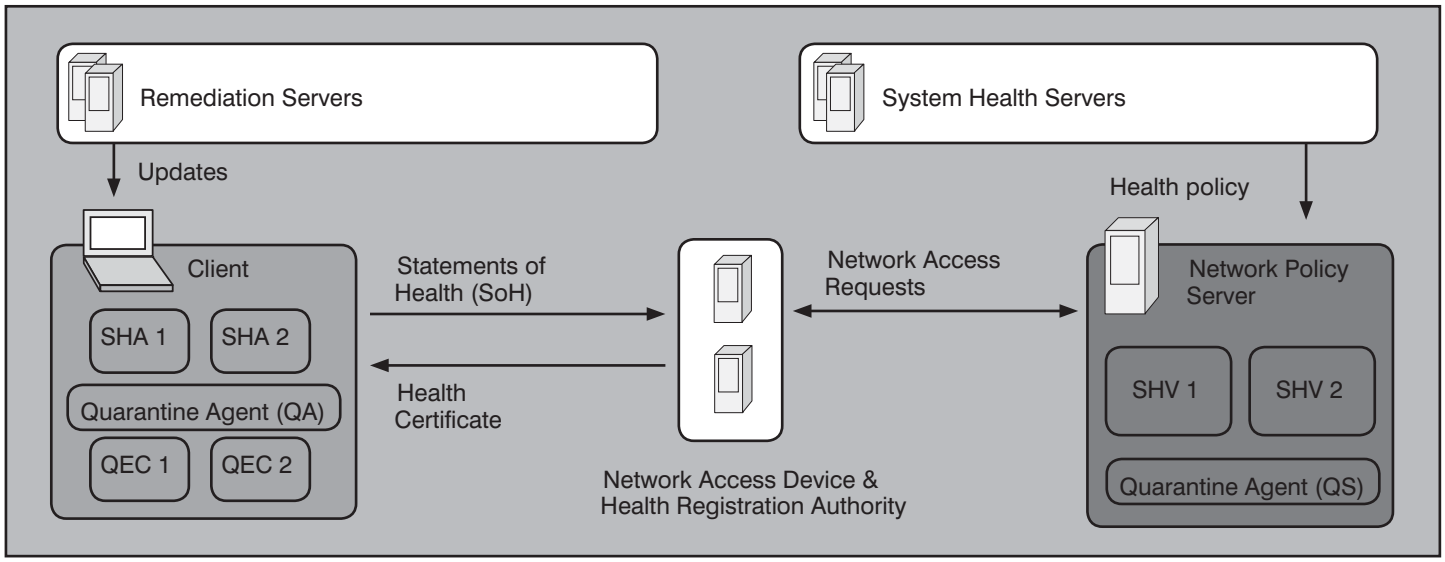


Abbildung 2: Steuerung via Radius Server (Quelle: Microsoft)

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,

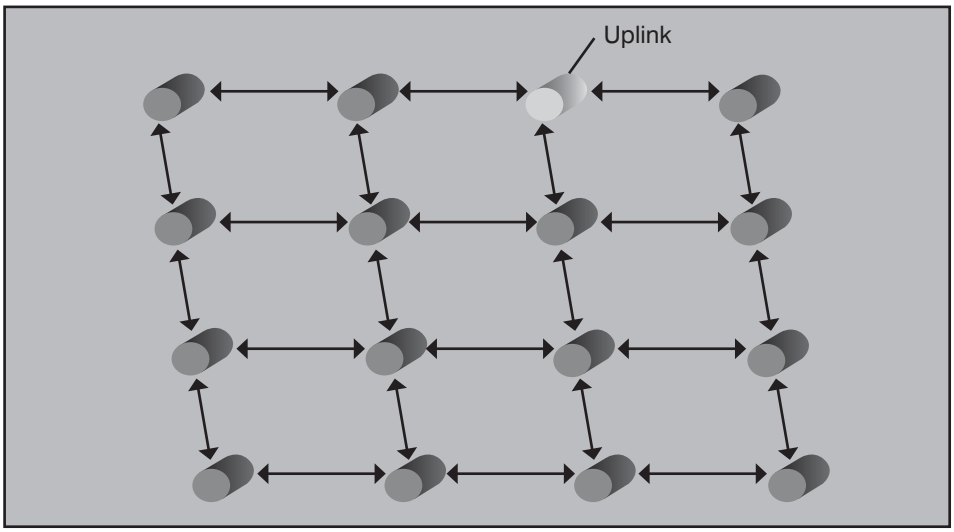


Abbildung 1: Maschen-Netz

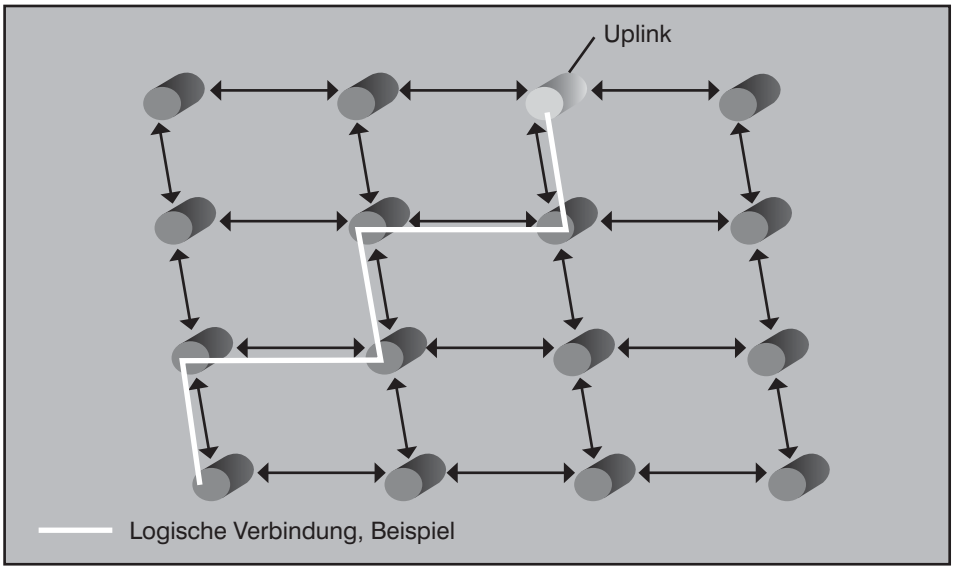


Abbildung 2: Maschen-Netz, Robustheit (1)

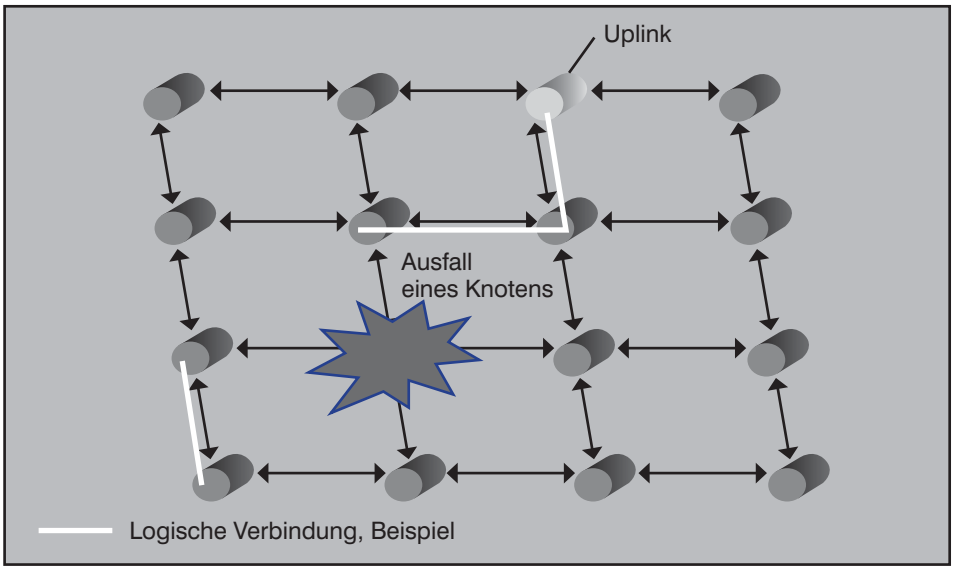


Abbildung 3: Maschen-Netz, Robustheit (2)

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