

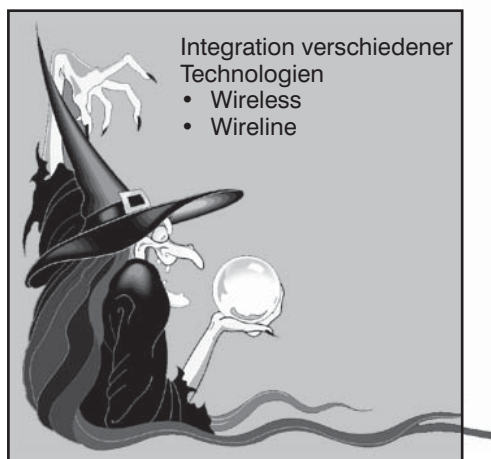
Schwerpunktthema

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends - Teil 2

von Dipl.-Inform. Petra Borowka

5. Weiterentwicklung: Vermaschte WLANS (Mesh WLANS)

Aktuell gibt es einen Weiterentwicklungstrend bei WLAN Herstellern hin zu einer verteilten, weitestgehend funkbasierten Architektur unter dem Namen „Vermaschtes WLAN“ (Mesh WLAN). Diese „Mesh Architektur“ benötigt nur noch wenige, bei Bedarf redundante Transit-Punkte vom drahtlosen zum drahtgebundenen Netz. Wie schon in Teil 1 unter dem Punkt „4. CAPWAP“ vermerkt, berücksichtigt auch CAPWAP das „Mesh WLAN“ zwar als separaten Architekturansatz, dessen Einbindung in CAPWAP durch die IETF Stand heute jedoch nicht weiter detailliert wird.



Eigentlich nahm die Entwicklung vermaschter WLANS ihren Anfang schon Mitte der 90er Jahre als Forschungsprojekt der DARPA für Schlachtfeld-Kommunikations-Szenarien, kurz darauf begannen Forschungs-Institute und -Unternehmen wie SRI International, sich mit diesem Thema zu befassen.

weiter auf Seite 22

Es bleibt spannend!

Zweitthema

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

von Dipl.-Inform. Matthias Egerland, Dr. Simon Hoff

Intrusion-Prevention-Systeme haben sich inzwischen im Portfolio der Maßnahmen zur Absicherung von Netzwerken etabliert. Dieser Artikel stellt die Funktionsweise solcher Systeme vor, zeigt am Beispiel von Snort-Inline die Erkennung eines Angriffs und diskutiert Einsatzszenarien, Aufbauvarianten und Marktsituation.

1. Die Grenzen eines klassischen stateful Paketfilters

Eine Firewall im Sinne eines zustandsbehafteten (stateful) Paketfilters kann Pakete richtungsabhängig Sitzungen (Sessions) zuordnen und anhand der Ports und IP-Adressen jeweils nach Quelle und Ziel filtern. Das Regelwerk des Paketfilters de-

finiert die erlaubten Kommunikationsbeziehungen, und was nicht erlaubt ist, wird verworfen. Die Welt wird dabei typischerweise in extern (untrusted bzw. unsicher) und intern (trusted bzw. sicher) eingeteilt und ein Sitzungsaufbau von extern nach intern nur im absoluten Ausnahmefall für spezielle Zielports und Ziel-IP-Adressen erlaubt.

weiter auf Seite 11

Top Veranstaltung

Gefahrenmelde- technik und Ob- jektüberwachung im Netz 2006

auf Seite 9

Zum Geleit

Kauf neuer Ether- net-Switches: schwierige Entscheidung

auf Seite 2

Report des Monats

Quality of Service in modernen Infrastrukturen

auf Seite 18

Zum Geleit

Kauf neuer Ethernet-Switches: schwierige Entscheidung

Relativ viele Netze, die im Rahmen der Jahr-2000-Welle erneuert worden sind, erreichen spätestens in diesem Jahr das Ende des üblichen Investitions-Intervalls. Zudem geben die Ende der 90er Jahre gegebenen MTBF-Zeiten Anlass, über Neuinvestitionen nachzudenken. Netzteile und Lüfter können je nach Produkt und Typ durchaus nach 6 oder 7 Jahren Betrieb zur Schwachstelle werden.

Und im Gegensatz zum PC, bei dem man vielleicht gelassen auf das Dahinscheiden wartet (vom Benutzer sehnlichst herbeigesehnt), geht es bei Netzwerk-Komponenten um Infrastruktur-Komponenten. Betroffen sind davon vor allem nicht modulare Switch-Komponenten. Modulare Switches können wie der Name schon sagt, ohne Probleme sowohl repariert als auch der aktuellen Technik angepasst werden (je nach Strategie des Herstellers).

So konzentriert sich der Neubeschaffungsbedarf der nächsten Jahre auch zu einem sehr hohen Prozentsatz auf den Etagen-/Workgroup-Bereich.

Parallel hat sich der Bedarf verändert. Überraschenderweise drückt sich das diesmal nicht in der Forderung nach höheren Datenraten aus sondern vielmehr in funktionalen Anforderungen. Dabei stehen die Bereiche Sicherheit und Power-over-Ethernet ganz oben.

Viele der zu ersetzenden Switch-Systeme sind 10 und 100 Mbit/s. In der Vergangenheit war es dabei fast ein Naturgesetz, dass mit dem Wechsel in die nächste Switch-Generation auch der Wechsel in die höhere Datenrate erfolgte. Demnach müsste der Wechsel in die Gigabit zum Endgerät schon fast selbstverständlich sein.

Dies ist es jedoch erstaunlicherweise nicht. Vergleicht man die Situation, die vor Jahren beim Wechsel von 10 auf 100 Mbit/s gegeben war mit der heutigen Situation, dann ist festzustellen, dass der Preisverfall bei Gigabit deutlich langsamer erfolgt und so der Preisabstand zwischen 100 Mbit/s und 1000 Mbit/s relativ hoch ist. Hinzu kommt, dass weiterhin nur wenige Anwendungen bekannt sind, die Gigabit wirklich



benötigen. Im Gegenteil, der Trend zum Datacenter im Web hat über die Schaffung neuer Software-Architekturen die Anforderungen an Datenraten je nach Bereich gesenkt. Die Beschaffung neuer Switches als 100 Mbit/s-Switches ist dann auch keine Seltenheit.

Die Situation ist dabei allerdings nicht so eindeutig wie das klingt. Mit der Reifung der Ethernet-Netzwerk-Technik hat parallel die Zahl der Anbieter zugenommen. Gerade im Bereich der nicht-modularen Etagen-Switches ist die Zahl der Anbieter unüberschaubar groß. Viele der in der Vergangenheit am Konsumermarkt orientierten Anbieter wie D-Link und Netgear sind inzwischen auch gut im Enterprise-Markt präsent. Damit ist eine gewaltige Spannweite an Preisen, Funktionalitäten und auch Qualität entstanden. Gerade im Bereich der MTBF-Zeiten lassen sich zum Beispiel noch klare Unterschiede zwischen den Herstellern feststellen.

Besonders der Einsatz von Power-over-Ethernet hat großen Einfluss auf den Preis. Zum einen unterscheiden sich hier die Anbieter, dann gibt es durchaus vereinzelte technische Probleme, zum anderen ist mit einem weiteren Upgrade des Standards in den nächsten Monaten zu rechnen (wobei die kommende Plus-Version des PoE-Standards für viele Anwendungen nicht zwingend einen Vorteil bringen wird).

Sollten die Switches 1:1 ausgetauscht werden oder sollten Änderungen in der Struktur vorgenommen werden?

Seit Ende der 90er Jahre hat sich vieles verändert. Die Möglichkeiten des Trunkings, die Zahl der Ports zur Verbindung zum Hauptverteiler, die Einführung von Rapid Spanning Tree und die weitere Ausdehnung von Layer-3-Bereichen bis in einzelne Etagen hinein sind Beispiele für mögliche Änderungen im Strukturbereich (so gibt zum Beispiel die Kombination aus Rapid Spanning Tree mit parallel erhöhten MTBF-Zeiten das Potenzial zur wirtschaftlich optimalen Maschenbildung).

Wohl die größte Herausforderung bei der Neubeschaffung von Switch-Systemen liegt im Bereich der zu schaffenden Sicherheits-Infrastruktur. Hier hat IEEE 802.1X einen signifikanten Mehrwert geschaffen.

Die Absicherung des Netzwerkzugangs durch Missbrauch vorhandener und beschalteter Dosen oder durch Missbrauch vorhandener PCs hat mit der höchsten Dringlichkeit in vielen Projekten. Besonders Netzwerke, die in Bezug auf das Bundesdatenschutzgesetz unter Nachweispflicht stehen, können nun so konfiguriert werden, dass jeder Zugriff dokumentiert werden kann.

Betrachtet man die vorausgegangenen Ausführungen, dann ist die Auswahl eines neuen Ethernet-Switches zur Ablösung der Altsysteme durchaus eine Herausforderung. Sie erfordert gute Marktkenntnisse, die neuen Strukturalternativen müssen beherrscht werden und im Bereich der neuen Sicherheitsverfahren gibt es noch nicht viel Erfahrungshintergrund.

Wir greifen diese Themen für sie auf. Zum einen auf dem Netzwerk-Redesign-Forum 2006, zum anderen auf unserer Sommerschule 2006. Beachten Sie auch das spezielle Seminar „Sicherheit im LAN mit IEEE 802.1X“, und den gerade erschienenen Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“ zu diesem Thema. Ich freue mich auf viele kontroverse Diskussionen.

Ihr
Dr. Jürgen Suppan

Top-Kongress

Netzwerk-Redesign Forum 2006

Die ComConsult Akademie veranstaltet vom 27. - 30. März das Netzwerk-Redesign Forum 2006.

Zum Netzwerk-Redesign-Forum 2006 präsentiert ComConsult-Research wieder eine Reihe exklusiver Analysen über die neuesten Entwicklungen, die Nutzbarkeit aktueller Technologien und Ansätze zur Betriebsoptimierung. Ergänzt wird dies um zahlreiche Vorträge von Top-Referenten und den abschließenden Intensiv-Tag.

Nachfolgend eine Auswahl der Analysen und Informationen, die Sie auf dem Redesign-Forum erwarten:

- Neueste Entwicklungen, was kommt auf Sie zu, wie wichtig ist es
- Netzwerk-Design und Produkt-Architekturen: wohin geht der Weg
- Betrieb von Netzwerken: wie sind weitere Verbesserungen zu erreichen?



- Sicherheit in Netzwerken: wie kann der Mega-GAU verhindert werden
- Ausgewählte Technologien in der Detailanalyse

Auch 2006 ist dies eine der wichtigsten und zentralen deutschen Netzwerk-Veranstaltungen.

Zögern Sie nicht, sich einen Platz auf dieser herausragenden Insider-Veranstaltung zu sichern.

Vertiefungstag

Unser Vertiefungstag bringt 3 brandneue und hochaktuelle Themenbereiche, die Sie auf keinen Fall verpassen sollten:

- SIP: Leistung, Stand der Entwicklung, Nutzbarkeit
- Wireless LAN in Produktion und Logistik
- Quality of Service: Projekterfahrungen zu Bedarf und Leistung

Moderation
Dr. Jürgen Suppan

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzwerk-Redesign Forum 2006

Ich buche den Kongress
Netzwerk-Redesign-Forum 2006
vom 27.03. - 30.03.06 in Königswinter

mit „Ein-Tages-Intensiv-Training“

- ☐ SIP: Leistung, Stand der Entwicklung, Nutzbarkeit
- ☐ Wireless LAN in Produktion und Logistik
- ☐ Quality of Service: Projekterfahrungen zu Bedarf und Leistung

zum Preis von € 2.190,- zzgl. MwSt.

☐ ohne „Ein-Tages-Intensiv-Training“

zum Preis von € 1.790,- zzgl. MwSt.

☐ mit Report

„Netzwerkdesign-Wettbewerb 2005“
zum Preis von nur € 210,- zzgl. MwSt.

☐ mit Report

„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
zum Preis von nur € 338,- zzgl. MwSt.

☐ ohne Report

- ☐ Bitte reservieren Sie für mich ein Hotelzimmer vom _____ bis _____ 06

Vorname

Nachname

Firma

Abteilung

Telefon

Fax

Straße

PLZ, Ort

eMail

Unterschrift



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

Programmübersicht: Netzwerk-Redesign Froum 2006

Montag, den 27.03.2006

9:30 bis 12:30 Uhr

Top-Analyse unseres internationalen Labors: Internationale IT-Trends und Auswirkungen auf Netzwerke und Infrastrukturen

- Neue IT-Architekturen und ihre Anforderungen
- Der Konsumer-Markt und seine Auswirkungen auf Client, Betriebssystem, Software
- Globalisierung und die Konsequenzen für Kommunikations-Architekturen
- Strategien ausgewählter Hersteller: Cisco, IBM, Microsoft, Siemens
- Moderne Technologien in der Trend-Analyse:
 - Speicher • Server/Datacenter
 - Intelligent Networks / Virtualisierung von Ressourcen im Netzwerk
 - IP-Telefonie • Kollaboration: Teamwork im Netzwerk
 - RFID, Architekturen und die Integrations-Aufgabe
 - Logistik-Anwendungen im Netzwerk
 - Aktuelle Netzwerk-Technologien und der Trend
 - Sicherheits-Architekturen für vernetzte Systeme
- Ausblick auf die internationale Entwicklung und die Konsequenzen für den deutschen Markt

Dr. Jürgen Suppan, ComConsult Research

14:00 bis 15:30 Uhr

Wireless-Technologien - wohin geht der Weg? Investitionssicherheit im Wettstreit von IEEE 802.11n und WiMax

- Aktuelle Wireless-Standards und ihre Vor- und Nachteile
- Konsumer- kontra Enterprise-Markt: wer bestimmt die Produkte
- IEEE 802.11n in der Analyse: Leistung und Grenzen eines neuen Standards
- WiMax: Vorteile der Wireless-Megatechnik
- IEEE 802.11n kontra WiMax: wohin geht der Weg

- Investitionssicherheit mit Wireless-Technologien: was ist zu tun?
- Wireless-Architekturen der Zukunft: die neue Wireless-Hierarchie
- Konsequenzen für die Zukunft: wie Netzwerke in 5 Jahren aussehen können
 - Campus-Design
 - Integration von Servern und Speicher
 - Distribution • Desktop-Bereich
- Fazit: Handlungsempfehlungen

Dr. Franz-Joachim Kauffels, Unternehmensberater

16:00 bis 17:30 Uhr

Netzwerk-Redesign 2006: Alternativen, Aufwand, Wirtschaftlichkeit

- Gründe für ein Redesign
- Bewertung bestehender Netzwerke und Designs
- Neue Technologien und ihr Einfluss auf Design-Entscheidungen
- Optimierung von Konvergenz-Zeiten
- Leistungsspektrum moderner Switch-Produkte
- Grundsätzliche Design-Alternativen
- Campus-/Backbone-Design im Umfeld konvergenter Netzwerke
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide in der Nutzbarkeits-Analyse
- Fallbeispiele und Empfehlungen

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

10:30 - 11:00 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

15:30 - 16:00 Uhr Kaffeepause

ab 18:00 Uhr Happy Hour

Dienstag, den 28.03.2006

9:00 bis 10:00 Uhr

Configuration Management Data Base CMDB:

Optimierung des Konfigurations-Managements von Netzwerken

- CMDB als Basis zentralisierter Konfigurations-, Sicherheits- und Management-Architekturen
- ITIL und CMDB: vom Leitfaden zur Lösung
- Praktische Anforderungen
- Alternativen zur Umsetzung
- Automatisierung als logische Folge:
 - Spezialthema Automatisierung: Generierung aus einer CMDB
 - Spezialthema Sicherheit: Zugangspflege der Netzwerk-Plattform automatisiert mit Hilfe der CMDB
 - Spezialthema Management: Konfigurationspflege der Management-Plattform auf Basis der CMDB
- Kosten und Betrieb
- Bewertung und Ausblick

Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik GmbH

10:00 bis 10:30 Uhr

Standardisierung und Technologie-Entwicklung:

- Was passiert aktuell bei IEEE, was ist neu, wie relevant ist es?
- Positionen der Hersteller
- Aktuelle Standardisierungs-Arbeiten
 - 802.3an 10GBASE-T • 802.3aq 10GBASE-LRM
 - 802.3as Frame Extension • 802.3at Power over Ethernet
 - 802.3ap Backpanel Ethernet
 - 802.3ar Congestion Management
 - Residential Ethernet
- Einschätzungen und Empfehlungen

Dipl.-Ing. Thomas Schramm, Hirschmann GmbH

11:00 bis 11:45 Uhr

Anforderungen an die Netzwerk-Infrastruktur für 10 Gig-Ethernet und für zukünftige Anwendungen

- Stand der Normierung
- Problematik bei der Umsetzung
- Empfehlungen

Stefan Ries, Reichle & De-Massari AG

11:45 bis 12:30 Uhr

WAN-Planung und Optimierung

- Neue WAN-Verfahren und ihre Bedeutung
- MPLS: Projekterfahrungen
- Applikationen und Datacenter im WAN
- Trends und Ausblick

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

14:00 bis 15:30 Uhr

Neue Wireless LAN-Technologien in der Analyse:

Projekterfahrungen

- Controller-basierte Architekturen kontra traditionelles Access-Point-Design
- Herausforderung: zentralisierte Konfiguration
- Konsequenzen für das Distributions-System und die WLAN-Sicherheits-Infrastruktur
- Markt- und Produktsituation Wireless-Switching
- Mobilität und Sicherheit: wie aufwendig ist IEEE 802.11i
- Empfehlungen für erfolgreiche und investitionssichere Wireless-Projekte

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:00 bis 17:00 Uhr

Sicherheit im Netzwerk: Zugriffsschutz auf Benutzerebene

- Bedrohungsanalyse
- Zugriffsschutz im Netzwerk: alternative Lösungsansätze
- Bestehende Standards und ihre Nutzbarkeit
- Potenziale und Grenzen gruppenbezogener Zugriffsrechte
- Praktische Umsetzung und Einsatzszenarien
- Behandlung von Problem-Geräten
- Prüfung der Patch-Level von Clients: Hersteller-Konzepte in der Bewertung
- Ausblick und Empfehlungen

Markus Schaub, ComConsult Technologie Information GmbH

10:30 - 11:00 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

15:30 - 16:00 Uhr Kaffeepause

Programmübersicht: Netzwerk-Redesign Froum 2006

Mittwoch, den 29.03.2006

9:00 bis 10:00 Uhr

Projekterfahrungen zur IP-Telefonie

- Vorgehensweise bei Ausschreibungen
- Applikationen und Sonderanwendungen in einer VoIP-Umgebung
- Voice-Tauglichkeit bestehender Netzwerke
- QoS-Konzeptionierung
- Welche QoS-Architektur ist zu empfehlen
- Integration und Trennung von Sprache und Daten im Netzwerk
- Ergebnisse aktueller Ausschreibungen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr

Business-Case IP-Telefonie

- Typischer Projektablauf: was gehört zum typischen Voice-Projekt, wo liegen Stolpersteine, welcher Zeitablauf ist realistisch
- Traditionelle TK kontra IP-Telefonie: was zeigen aktuelle Projekterfahrungen
- Wirtschaftlichkeit: Ergebnisse aktueller TCO-Berechnungen, typische Amortisationszeiten
- Hosted IP-Telefonie: eine Alternative?
- Markt-Analyse: wo stehen wichtige Hersteller, welche Strategien verfolgen sie, wer ist für die nächsten Jahre am besten aufgestellt
- Sind offene, standardisierte Lösungen realisierbar?
- Zeitlicher Ausblick: was dominiert die nächsten 3 Jahre
- Empfehlungen für die erfolgreiche Projektdurchführung

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

11:30 bis 12:30 Uhr

Mobile Kommunikation

- Anwendungsszenario mobile Kommunikation
- Aktuelle Standards: was sie leisten, was sie nicht leisten
- Herausforderung: zentrales Management der mobilen Endgeräte
- Integration in bestehende Strukturen (Active Directory, Exchange)
- Spezifische Sicherheitsanforderungen an mobile Endgeräte
- Sicherheit versus Nutzungskomfort

- Marktanalyse: welche Softwarelösungen gibt es und was sie leisten
- Welche Leistungsmerkmale sind unverzichtbar
- Trends und Ausblick

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

14:00 bis 14:45 Uhr

Integration von Gefahren- und Meldetechnik in IP-Netzwerke

- Das universelle Gefahrenmeldenetz, baldige Realität oder bleiben es zwei Welten
- Videoüberwachung im Netzwerk: Motivation, Trends und Produkte
- Anforderungen an das Netz zur Einführung von Videoüberwachung
- Aufbau von „Video-Netzwerken“
- Video over Wireless
- Gefahrenmeldetechnik im LAN: Probleme und Lösungen
- Anforderungen der Sicherheitstechnik und Anforderungen an die Verfügbarkeit
- Trends und Ausblick

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

15:15 bis 16:00 Uhr

IPS und Firewalls: Ergänzung oder Konkurrenz

- Funktionsweise eines Intrusion Prevention Systems (IPS)
- Techniken zur Erkennung von Angriffsmustern
- Netzbasierende und Host-basierte Systeme
- Abgrenzung zu Firewall-Systemen
- Einsatzvarianten und Architekturen
- Produktsituation

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

14:45 - 15:15 Uhr Kaffeepause

Donnerstag, den 30.03.2006 - Ein-Tages-Intensiv-Trainings/Workshops - Beginn 09:00 Uhr

BITTE EIN GEWÜNSCHTES THEMA ANKREUZEN!!**Intensiv-Training 1:****SIP in der Analyse:****auf dem Wege zur offenen IP-Telefonie?**

- Was leistet SIP, wie arbeitet es?
- Welche Komponenten werden benötigt?
- Wie sehen typische Produkte aus?
- Ein Alltags-Szenario und seine Umsetzung mit SIP
- Variante 1: die offene Lösung
- Variante 2: SIP und die traditionellen Hersteller
- Ausblick

Markus Schaub, ComConsult Technologie Information GmbH

**Intensiv-Training 2:****Wireless LAN in Produktion und Logistik**

- Spezielle Anforderungen in Produktions- und Logistik-Umgebungen
- Wireless-Technologien und ihre Nutzbarkeit
- Roaming-/Handover
- Umsetzung hoher Verfügbarkeit und Redundanz
- Problem der WLAN-Ausleuchtung
- Echtzeitanforderungen für WLAN-Anwendungen: Möglichkeiten und Grenzen
- Integration von Altlasten und von unsicheren Endgeräten
- Umgang mit Störungen
- Access Points für Industrieumgebungen
- Beispiele und Projekterfahrungen
- Ausblick und Empfehlungen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Bitte wählen Sie vorab ein Intensiv-Training aus, damit wir die weitere Organisation planen können. DANKE!

**Intensiv-Training 3:****Quality of Service**

- QoS-Ziele
- QoS-Anforderungen in Lokalen Netzwerken
- QoS-Mechanismen
 - Auf Ethernet-Ebene
 - Auf IP-Ebene
 - Über IP-Ebene
- Konzepte für den LAN-Ausbau im Hinblick auf QoS
 - Access-Bereich
 - Core-Bereich
 - Back-End-Bereich
- Sonderfall: QoS und IP-Telefonie
- Messungen in produktiven Netzwerken
 - Aufbau
 - Ergebnisse
- QoS im WAN
 - Architektur
 - Flankierende Maßnahmen
 - IP-Telefonie im WAN
- QoS im Wireless LAN
 - Einfluss der WLAN-Technologie
 - Kanalzugriff und Handover
 - IP-Telefonie
- Fazit und Empfehlungen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

13:00 - 14:00 Uhr Mittagspause

15:30 Ende der Veranstaltung

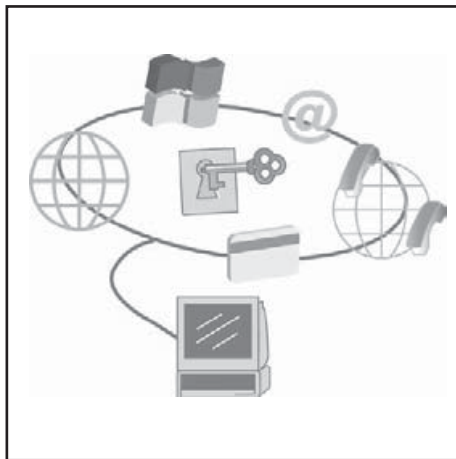
IT-Sicherheits-Kongress

IT-Sicherheits-Forum 2006

Die Comconsult Akademie veranstaltet zusammen mit der GAI NetConsult Berlin vom 08. - 11. Mai das „IT-Sicherheits-Forum 2006“ in Bad Neuenahr.

Das Programm dieses hochaktuellen Sicherheits-Kongresses besteht aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen. Das Forum verbindet die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Am 1. Tag folgenden Tutorien jeweils mit Live-Demos durchgeführt:



1. Übersicht zu aktuellen Themen der IT-Security
2. VoIP-Security - Sicherheitsprobleme und rechtliche Situation
3. Layer-2 Security - Technologie, Bedrohungen, Schutzmaßnahmen

Am 3. Tag werden in parallelen Sessions stark praxisorientierte Workshops durchgeführt. Dazu gehören moderierte Produktvergleiche (u.a. zu Content Security Gateways, Application Firewalls) ebenso wie die gemeinsame Erarbeitung von Lösungsszenarien (u.a. für Notfallkonzepte, Sicherung kritischer Infrastrukturen, sichere Adminumgebungen).

Fax-Antwort an ComConsult 02408/955-399

Anmeldung IT-Sicherheits-Forum 2006

Ich buche den Kongress **IT-Sicherheits-Forum 2006** vom 08.05. - 11.05.06 in Bad Neuenahr

mit Tutorium am ersten Tag

☐ Thema 1 ☐ Thema 2 ☐ Thema 3
zum Preis von nur € 2.190,- zzgl. MwSt.

☐ ohne Tutorium am ersten Tag

zum Preis von nur € 1.790,- zzgl. MwSt.

Workshopauswahl am 10.05.06

vormittags

- ☐ Workshop 1
☐ Workshop 2
☐ Workshop 3
☐ Workshop 4

nachmittags

- ☐ Workshop 3
☐ Workshop 5
☐ Workshop 6

☐ **mit Report**

„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“

zum Preis von nur € 338,- zzgl. MwSt.

☐ **ohne Report**

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom _____ bis _____ 06

Vorname

Nachname

Firma

Abteilung

Telefon

Fax

Straße

PLZ, Ort

eMail

Unterschrift



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

Programmübersicht IT-Sicherheits-Forum 2006

Montag, 08.05.06 Tutorien

**Alle Tutorien finden parallel statt und starten um 10:00 Uhr und enden gegen 17:30 Uhr.
Bitte wählen Sie Ihr bevorzugtes Tutorium aus. (Anmeldung)**

Tutorium 1: Aktuelle Themen der IT-Security - Angriffe, Konzepte, Lösungen im Überblick (mit Live-Demo)

- **Vorstellung realer Angriffsszenarien**
- **Grundlagen der IT-Sicherheit**
Umgang mit Risiken, Schutzziele, Elementare Maßnahmen
Security Policy, Grundschutz, BS 7799
- **Grundlagen der Verschlüsselungstechnologie**
Einführung, Kryptografie, aktuelle Standards
- **Lösungen zur E-Mail Sicherheit**
Client-Plug-Ins, Gatewaylösungen
- **Von Firewall bis VPN**
Konzepte, DMZ, Betrieb, Praxis
- **Sicherheitsfunktionen von Windows 2003/XP**
Distributed Security Services, SmartCards
- **Sichere Server**
Logging, Backup, Hardening
*Hans-Joachim Knobloch,
Secorvo Security Consulting GmbH*

Tutorium 2: VoIP-Security Technische und Rechtliche Sicherheit (mit Live-Demo von Angriffen)

- **Kurzvorstellung VoIP**
- **Gefahren bei der Nutzung von VoIP**
Angriffe gegen VoIP-Kommunikation
Bedrohungen durch Verwendung dynamischer Ports
- **Transport von Malware über VoIP-Protokolle**
- **Angriffe auf Handy- und WLAN-Funkstrecken**
- **Rechtliche Sicherheit bei VoIP**
Fernmeldegeheimnis und Betriebsverfassungsrecht
- **Sicherheitsanforderungen an VoIP**

*Ulrich Emmert, Frank Gebert
esb Rechtsanwälte*

Tutorium 3: Layer-2 Security - Angriffe gegen die Netzwerk-Infrastruktur (mit Live-Demo von Angriffen und Tools)

- **Überblick zu Layer-2 Technologien und Protokollen**
- **Vorstellung der wichtigsten Sicherheitsprobleme**
- **Layer-2 Security Features (Private VLANs, DHCP Snooping, ARP Inspection, 802.1X)**
- **Ausblick auf moderne WAN-Technologien (Metro Ethernet, Ethernet over MPLS, Virtual Private LAN Services)**
- **Auswirkungen auf die Layer-2 Security**

*Enno Rey
ERNW Netzwerke GmbH*

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause

Dienstag, 09.05.06

10:00 Uhr – 10:15 Uhr Begrüßung/Übersicht

*Detlef Weidenhammer,
GAI NetConsult GmbH*

10:15 Uhr – 11:00 Uhr

Sicherer Umgang mit modernen Kommunikationsformen

- Instant Messaging: Von ICQ bis Jabber - Nutzen oder verbieten?
- Peer-to-Peer: von eDonkey bis Bittorrent - was geht davon im Unternehmen?
- Anonymisierungsdienste im Unternehmen: Datenschutz gegen IT-Sicherheit?
- Von http-Tunnel bis JAP: Warum überhaupt noch eine Firewall?

*Prof. Dr. Rainer W. Gerling
Max-Planck-Gesellschaft*

11:00 Uhr – 11:45 Uhr

Zunehmende Kriminalisierung des Internet

- Massenhaft vorgetragene Angriffe (Phishing, Botnets usw.)
- Gezielte Angriffe mit Spyware
- Attacken auf kritische Infrastrukturen
- Abwehrmaßnahmen

*Detlef Weidenhammer,
GAI NetConsult GmbH*

12:15 Uhr – 13:00 Uhr

IT-Sicherheit in kritischen Infrastrukturen

- Einführung in die Thematik „Kritische Infrastrukturen“
- Nationale und internationale Aktivitäten
- KRITIS-Materialien des BSI
- Sicherheitsrichtlinie und -check in der Praxis

*Stefan Gunzelmann,
consequa GmbH*

14:30 Uhr – 15:15 Uhr

Sicherheitszonen in der LAN-Infrastruktur

- Seiteneffekte konvergenter Netze auf die Sicherheit
- Sicherheitsinfrastrukturen bei Gefährdungen von innen
- Firewalls und Protokolle in verteilten Systemen
- Authentifizierung und Autorisierung am LAN-Zugang:
Techniken und ihre Grenzen
- Zugang für Gäste und Fremdfirmenmitarbeiter

*Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH*

15:15 Uhr – 16:00 Uhr

Entwicklung eines Konzepts für Security Incident Handling

- Einbettung des Security Incident Handlings in die vorhandenen Prozesse (Sicherheitsprozess, Business Continuity, Disaster Recovery)
- Komponenten des Security Incident Handlings und Berücksichtigung der verschiedenen Bedrohungsphasen
- Definition eines Security Incident Handling Prozesses
- Erfahrungen bei der Umsetzung

*Sven Schumann,
HUK-Coburg-Allgemeine Versicherung AG*

16:30 Uhr – 17:15 Uhr

Business Continuity Planing in der IT-Praxis

- Einführung in die BCP-Thematik
- Einsatz eines Scoring-Verfahrens bei der Bestimmung kritischer Prozesse
- Notfallpläne und ihre Praxistauglichkeit
- Test, Pflege und Revision der Planung

*Holm Dienes,
GAI NetConsult GmbH*

17:15 - 18:00 Uhr

Security Awareness - Mitarbeitersensibilisierung

- Mitarbeiter als „letzte Bastion“ der IT-Sicherheit
- Das 4-Phasen-Konzept einer Awareness-Kampagne
- Zentrale Erfolgsfaktoren
- Praxisbeispiele

*Dirk Fox,
Secorvo Security Consulting GmbH*

11:45 - 12:15 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Programmübersicht IT-Sicherheits-Forum 2006

Mittwoch, 10.05.06 Praxis-Workshops - Die Durchführung der Workshops wird am Teilnehmerinteresse ausgerichtet.

Workshops 09:00 - 12:30 Uhr

Workshop 1:

Einsatz von netzwerk-basierten IPS

- IPS versus IDS und Abgrenzung zu Firewall: Motivation für IPS
- Funktionsweise von IPS: Techniken zur Erkennung von Angriffen
- Aufbaukonzepte, Redundanz und Performance
- Zu beachtende Aspekte bei der Auswahl von IPS
- Produktbeispiele
- Praktische Erfahrungen

Dr. Simon Hoff,

ComConsult Beratung und Planung GmbH

Workshop 2:

Modern Hacking - Know your Enemy

Live-Demo von Angriffstechniken

- Schwachstellentrends 2005 / 2006
- Passive Zielfindung per Suchmaschine (Google-Hacking und Co.)
- Moderne Exploittechniken und -frameworks
- Angriffe auf Applikationsebene
- Rootkits und Anti-Forensics

Björn Fröbe,

GAI NetConsult GmbH

Workshop 3:

Business Continuity Planing im IT-Umfeld

Live-Demo eines Tools

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege

- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

Holm Diening,

GAI NetConsult GmbH

Workshop 4:

Sicherheit von BlackBerry und Alternativlösungen - Vergleich unterschiedlicher Lösungen

- Einführung und Überblick zu den im Workshop vertretenen Produkten
- Sicherheitsaspekte einer Mobile PIM-Lösung:
- Schutz der Endgeräte
- Schutz der Kommunikation
- Schutz der zentralen Server
- Zentrales Management und Überwachung
- Live-Demonstrationen der verschiedenen Lösungen
- Auswahlkriterien für die eigene Produktauswahl

Frank Breitschaft,

GAI NetConsult GmbH

Workshops 14:00 - 17:00 Uhr

Workshop 5:

IT-Security Best Practice

Top-10 Tips und Tricks in der Diskussion

Vorgesehene Themen sind:

- Konfiguration von Webbrowsern
- Sicherung von Webservern
- Sichere E-Mail
- Aufbau einer sicheren Adminumgebung
- VPN (IPsec und SSL)
- Secure RAS

Björn Fröbe, Dr. Torsten Johr,

GAI NetConsult GmbH,

Dr. Simon Hoff, Andreas Meder,

ComConsult Beratung und Planung GmbH,

Workshop 6:

Intelligente Analyse von Security Log Files

- Security Log File Korrelation mit Aufzeichnung und Rekonstruktion kritischer Ereignisse
- Welche Art der Event-Korrelation macht Sinn?
- Anforderungen an einen Tool-Einsatz
- Vorgehensweise bei der Suche nach „Critical Events“
- Ergänzung forensischer Untersuchungen
- Nutzung der Erkenntnisse auch für Basel II, Sarbanes-Oxley etc.
- Praktische Beispiele und Hands-On

Paul Hoffmann,

DATAKOM GmbH,

Peter Weinlich,

GTEN AG

Workshop 3:

Business Continuity Planing im IT-Umfeld

Live-Demo eines Tools

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege
- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

Holm Diening,

GAI NetConsult GmbH

11:00 - 11:30 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

16:00 - 16:30 Uhr Kaffeepause

Donnerstag, 11.05.06

9:00 Uhr - 10:00 Uhr

Projektbericht: IT-Sicherheit nach BS 7799

- Ziel: Beratung zu organisatorischen und strategischen IT-Sicherheitsmaßnahmen
- Anwendung von ISO-Standard 17799 und BS 7799-2
- Pflichtenheft, IT-Assessment, Risikoanalyse
- Erstellung von Security Policy, Notfallkonzept und Sicherheitshandbuch

Frank Spanier,

DKV Euro Service GmbH & Co KG,

Stefan Schänzer,

BDG GmbH & Co KG

10:00 Uhr - 11:00 Uhr

Prozessorientiertes IT-Sicherheitsmanagement mit ITIL

- ITIL: die Vorstellung
- Der Prozess ITIL Security Management
- Maßnahmen und Implementierung
- Koexistenz mit ITSM-Standards

Christian Aust,

.consecro

11:30 Uhr - 12:30 Uhr

Projektbericht: Aufbau eines sicheren Extra-net-Webportals

- Projektstart: Business vs. Security Requirements
- Durchführung einer Risikoanalyse
- Aufbau einer Schutzlösung mit Web Application Firewall und Access Management
- Aufbau der zugehörigen Sicherheitsorganisation

Martin Noll,

Schering AG

13:45 Uhr - 14:45 Uhr

Evaluierung von Web Application Firewalls

- Evaluierungskriterien des Web Application Security Consortiums
- Überblick zu den am Markt verfügbaren Produkten
- Bewertung und KO-Kriterien in einzelnen Szenarien
- Hinweise für die eigene Produktauswahl

Frank Breitschaft,

GAI NetConsult GmbH

14:45 Uhr - 15:45 Uhr

Sicherheit für service-orientierte Architekturen (SOA)

- SOA - ein Überblick
- Technische Grundlagen: XML Web Services, Architekturprinzipien
- Umsetzung von SOA-Sicherheit
- Vorstellung eines Fallbeispiels

Dr. Sebastian Staamann,

PrismTech GmbH

15:45 Uhr

Zusammenfassung und Schlusswort

Detlef Weidenhammer,

GAI NetConsult GmbH

11:00 - 11:30 Uhr Kaffeepause

12:30 - 13:45 Uhr Mittagspause

16:00 Uhr Ende der Veranstaltung

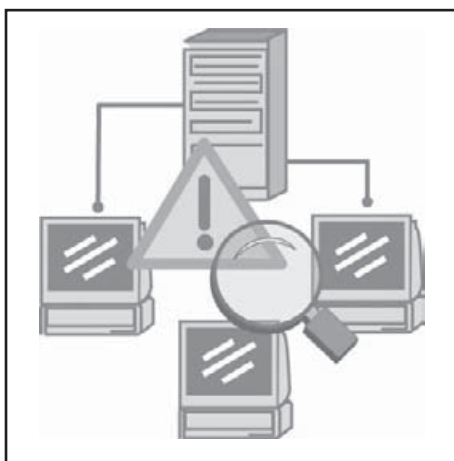
Frühjahrs-Kongress

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Die Comconsult Akademie veranstaltet vom 15. - 16. Mai das „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ in Köln.

Der Ruf nach konvergenten Netzen macht vor dem Bereich der Gefahren- und Meldetechnik nicht halt, die Nachfrage nach einer Nutzungsmöglichkeit von IP-basierenden Netzen für Videoüberwachung, Einbruchmeldetechniken, Brandmelder, Zutrittskontrollen und ähnlichem nimmt rapide zu. Sowohl auf der Seite der klassischen Gebäudeüberwachungstechnik wie auch bei den IT-Spezialisten herrscht Unsicherheit darüber, welche dieser klassischen Techniken bereits heute durch IP abgedeckt werden können.

Das ComConsult-Forum „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ führt die bereits 2005 im gleichnamigen Forum begonnene Analyse der Technologie-, Markt- und rechtlichen Si-



tuation fort, und gibt wesentliche Empfehlungen zur Einführung dieser neuen Techniken. Neben der Überarbeitung der Themen des Forums von 2005 werden vollkommen neue Themen Gegenstand der Veranstaltung sein.

Dieses Forum bietet die ideale Basis für eine Standortbestimmung. Wer immer beabsichtigt in Gebäuden eine IP-basierende Gefahrenmeldetechnik bzw. Objektüberwachung einzuführen oder sein Netz darauf vorzubereiten, der sollte dieses Forum nicht verpassen.

Moderation

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 15-jährige Berufserfahrung in Datenkommunikation in lokalen Netzen verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Ich buche den Kongress
**Gefahrenmeldetechnik und
Objektüberwachung im Netz 2006**
vom 15.05. - 16.05.06 in Köln

☐ **mit Report**
„Ethernet in Industrie-Umgebungen“
zum Preis von nur € 338,- zzgl. MwSt.

☐ **ohne Report**

☐ Bitte reservieren Sie für mich
ein Hotelzimmer

vom _____ bis _____ 06

Vorname _____

Nachname _____

Firma _____

Abteilung _____

Telefon _____

Fax _____

Straße _____

PLZ, Ort _____



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

eMail _____

Unterschrift _____

Programmübersicht Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Montag, den 15.05.2006

10:00 bis 11:15 Uhr

Integration von Gefahrenmanagement in IP-Netzen: Probleme und Lösungen

- Schwachstellen von IP-Netzen hinsichtlich Verfügbarkeit, Sicherheit, Echtzeitfähigkeit
- Welche Netzstrukturen bieten die höchste Verfügbarkeit?
- Erhöhung der Sicherheit von IP-Netzen
- Verfahren für die Trennung verschiedener Anwendungen in der selben Netzinfrastruktur
- Wie können in IP-Netzen garantierte Übertragungszeiten sichergestellt werden?

*Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

11:45 bis 12:30 Uhr

Integrationsmöglichkeit von Fremdgewerken

- Wichtige Basisfunktionen
- Einsatzschwerpunkte: Was muss, sollte und kann integriert werden (EMA, GLT, BMA, Video usw.)
- Schnittstellenproblematik (herstellerspezifische, OPC, Bacnet, SNMP, Patientenruf)
- Alarmbehandlung
- Sondersysteme (reine Alarmserver) Produkte wie DAKS und NewVoice
- Entscheidungshilfen und Herstellerübersicht

*Dipl.-Ing. Holger Häntzschel,
SSMB Service-, Sales und Managementberatungs GmbH*

12:30 bis 13:15 Uhr

Netzbasierende Gefahrenmeldetechnik (Brand/Einbruch)

- Lassen aktuelle Normen Netzwerklösungen zu?
- Kocht jeder sein eigenes Süppchen?
- Wie kommen Gefahrenmeldungen ins LAN?
- Welche Funktionen einer Gefahrenmeldeanlage sind netzwerkfähig?
- Entwicklung und Trends

*Peter Loibl,
VON ZUR MÜHLEN'SCHE GmbH*

14:45 bis 15:30 Uhr

Integrale Gefahrenmanagementsysteme? Alles ist möglich, was ist sinnvoll?

- Realisierungskonzept eines Gefahrenmanagementsystems
- Wirtschaftlichkeitsbetrachtung
- Intuitive Bedienerinterfaces und effektive Systempflege
- Ereignisgesteuertes Notfallmanagement und Protokollierung
- Herstellerneutrale Integration von bestehenden Anlagen
- Praxisbeispiele aus verwirklichten Objekten
- Live Systemdemonstration einer typischen Anwendung

*Lothar Marth,
Novar GmbH by Honeywell*

15:30 bis 16:30 Uhr

Quality of Service im Dienste von Gefahrenmanagement

- Warum ist Quality of Service im Zusammenhang mit Gefahrenmanagement wichtig?
- Gesamtarchitektur für Quality of Service
- Quality of Service in drahtgebundenen LAN
- Quality of Service in Wireless LAN
- Quality of Service in WAN

*Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

17:00 bis 17:45 Uhr

Videoüberwachung über IP (Anforderungen, Lösungen, Grenzen)

- Motivation
- Anforderungen an die Video-Qualität
- Welche Funktionen können implementiert werden?
- Anforderungen an das Netz
- Aufbau von „Video-Netzwerken“

*Dipl.-Ing. Hartmut Kell,
ComConsult Beratung und Planung GmbH*

11:15 - 11:45 Uhr Kaffeepause

13:15 - 14:45 Uhr Mittagspause

16:30 - 17:00 Uhr Kaffeepause

ab 18:00 Uhr Happy Hour

Dienstag, den 16.05.2006

9:00 bis 10:00 Uhr

Sicherheitsanforderungen von Gefahrenmeldelösungen in Lokalen Netzwerken und ihre Umsetzung

- Bedrohungen im LAN und Auswirkungen auf Gefahrenmeldesysteme
- Sicherheitsmaßnahmen für die Übertragung der Überwachungs- und Melde-daten
- Verschlüsselung und Authentifizierung: Was muss sein und was ist überhaupt sinnvoll möglich?
- Schutz der Komponenten und der Übertragungswege eines Gefahrenmeldesystems

*Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH*

10:00 bis 10:30 Uhr

Praktische Umsetzung von Videoüberwachung über IP (Projektbeispiel)

- Was war die Motivation für Video über IP?
- Welche Anforderungen an die Video-Qualität wurden gestellt?
- Welche Funktionen wurden implementiert?
- Welche Anforderungen haben wurden an das IP-Netz gestellt
- Wie wurde das „Video-Netzwerk“ aufgebaut?
- Anforderungen an die Video-Qualität

*Firma tfa,
N.N.*

11:00 bis 11:30 Uhr

Vortrag des VdS (unter Vorbehalt)

- Wie sieht der VdS die kommende Nutzung von Lokalen Netzen für sicherheitsrelevante Applikationen wie z.B. Videoüberwachung, Brandmeldetechnik, Zugangskontrolle etc.?
- Gibt es schon eine Berücksichtigung dieser Ideen bei der VdS-Zertifizierung? Wenn ja welche?
- Welche Anforderungen muss man an die Infrastruktur stellen, um solche Zertifizierungen zu erhalten?
- Arbeitet der VdS bereits mit anderen Prüfungs- bzw. Zertifizierungsgremien wie z.B. dem TÜV zusammen?

N.N.

11:30 bis 12:15 Uhr

Intercom over IP

- IoIP® - Intercom over IP - Möglichkeiten, Unterschiede, Lösungen

- Was ist Intercom over IP?
- Unterschiede zu Telekommunikationstechniken (IoIP/VoIP)
- Lösungsbeispiele

*Harald Weber,
SCHNEIDER INTERCOM GmbH*

13:30 bis 14:45 Uhr

Funküberwachung: Stabilität, Verfügbarkeit, Sabotierbarkeit

- Was leisten die Datendienste der Mobilfunknetze (GSM/GPRS, UMTS) und welche Einsatzbereiche sind sinnvoll
- Bluetooth und WLAN in der Funküberwachung
- Sicherheit in Funknetzen
- Stand der Dinge bei ZigBee

*Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH*

14:45 bis 15:30 Uhr

Vortrag eines marktführenden Herstellers von Gefahrenmeldesystemen

- Anforderungen
- Berücksichtigung von vorhandenen Strukturen
- Nutzung kundeneigener Datennetze für sicherheitsrelevante Meldungen über IP (Projektbeispiele)

N.N.

15:30 bis 16:15 Uhr

Nutzeranforderungen zu Gefahrenmeldesystemen im RZ

- Raumüberwachung (Einbruchmeldeanlage, Türüberwachung, Kameras, Brand/Rauch, Temperatur, rel. Luftfeuchte, Wasser)
- Infrastrukturüberwachung (Klimaanlage, Stromversorgung, USV, Notstrom)
- Professionelle Lösungen für große RZ
- Kleine Lösungen für kleine RZ und wichtige Technikräume

*Mark Groten,
ComConsult Beratung und Planung GmbH*

10:30 - 11:00 Uhr Kaffeepause

12:15 - 13:30 Uhr Mittagspause

ca. 16:15 Ende der Veranstaltung

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

Fortsetzung von Seite 1



Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb im Bereich lokaler Netze, mobiler Kommunikationssysteme und deren Anwendungen zurück.



Dipl.-Inform. Matthias Egerland hat an der RWTH Aachen Informatik studiert und ist seit 2005 Mitarbeiter der ComConsult Beratung und Planung GmbH. Als Mitglied des Competence Center IT-Sicherheit beschäftigt er sich insbesondere mit der Sicherheit in LAN- und WAN-Umgebungen. In Projekten beteiligt sich Herr Egerland darüber hinaus an Konzeptionierungen und Ausschreibungen von IT-Infrastruktur-Lösungen in den Bereichen Virtual Private Networks (VPN), Metropolitan Area Networks (MAN) sowie konvergenten Netzen.

Solche Ausnahmen könnten beispielsweise ein Zugriff auf einen Web-Server in einer DMZ oder auf einem VPN Gateway sein.

Eine solche Firewall reduziert die Angriffsfläche immens, denn ein Angriff muss sich notgedrungen auf erlaubte Kommunikationsbeziehungen beschränken.

Das alleine reicht natürlich oft nicht aus. Zunächst kann ein Angreifer einen offenen Port ausnutzen und versuchen, etwa durch bewusst fehlerhaft formatierte Anwendungspakete einen Pufferüberlauf im angegriffenen Zielsystem zu erreichen. Über diesen Weg kann nun eine kleine Codesequenz in das Zielsystem eingeschleust werden, das nun willenlos die Codesequenz ausführt und so mehr oder weniger vollständig kompromittiert wird. Am Ende ist das angegriffene Zielsystem etwa mit einem Wurm oder einem Trojaner infiziert. Genauso kann das System eines unvorsichtigen Nutzers über eine erlaubte Kommunikationsbeziehung infiziert werden, etwa indem der Nutzer (trotz aller Ermahnungen) einen in einer E-Mail mit unbekanntem Absender angegebenen Link anklickt.

Es sind also in den meisten Fällen weitergehende Sicherheitsmechanismen erforder-

lich, zu denen beispielsweise der obligatorische Virenschutz und die Palette der Proxy-Lösungen und Application Layer Gateways gehören. Dies funktioniert auch recht gut, solange die Trennungslinie zwischen intern und extern scharf gezogen werden kann und nur in wenigen, effektiv kontrollierbaren Fällen der Übergang von extern nach intern gestattet wird.

Gerade hier liegt ein Problem: Je mehr Informationen zwischen Unternehmen, Organisationen und Behörden ausgetauscht werden, desto mehr verwischen naturgemäß die Grenzen zwischen intern und extern. Je komplexer die Kommunikationsbeziehungen im Netz sind, desto schwieriger ist es, alle Systeme rechtzeitig gegen Angriffe und speziell gegen schadenstiftende Software (Malicious Software, kurz Malware) zu schützen. Um den Betrieb aufrecht zu halten, kann es manchmal sogar notwendig sein, bestimmte Sicherheitslücken auch bei verfügbaren Patches offen zu lassen, weil wichtige Anwendungen auf einem gepatchten System nicht mehr korrekt funktionieren würden.

Hier sind es insbesondere die inzwischen unverzichtbaren Techniken so genannter Verteilter Systeme und hier speziell die verschiedenen Varianten von Remote Procedure Calls (RPCs), deren Sicherheitslücken

besondere Sorgen machen. Hierzu sei nur auf die unter <http://www.sans.org/top20/> veröffentlichte Liste der kritischsten 20 Sicherheitsschwachstellen hingewiesen. Ein signifikanter Anteil in dieser Liste bezieht sich auf RPC-Schwachstellen.

Ein interessantes Beispiel hierzu kann im Bereich der industriellen Fertigung gefunden werden, denn in modernen Maschinen finden sich häufig PCs unter MS Windows, die mit Kontroll- und Steuerungsaufgaben behaftet sind. Die Kommunikation geschieht dabei vermehrt basierend auf RPC-Mechanismen. Diese PCs sind Bestandteil der Maschine und daher meist nicht in die IT-Prozesse für Patch- und Virenschutzaktualisierung für Standard-PCs integriert. Solche PCs in Maschinen können leicht von einer Malware infiziert werden (beispielsweise durch das infizierte Notebook eines Service-Technikers, das zu Wartungszwecken an das LAN angeschlossen wird), so dass innerhalb von kürzester Zeit die Produktion stehen würde.

Hier stößt auch der klassische Virenschutz an seine Grenzen, denn diese Systeme sind zwar in der Lage, spezielle Infektionswege zu überwachen und dort die Signatur eines Virus zu erkennen, sie können aber meist nicht das Verhalten der Schadensroutine einer Malware (also das ei-

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

gentliche Angriffsverhalten) erkennen. In diesem Zusammenhang kann darüber nachgedacht werden, Systeme mit hohem Schutzbedarf durch eine Firewall von den anderen am LAN angeschlossenen Geräten zu trennen. Jedoch folgt hier mit der Komplexität der Kommunikation (Stichwort RPC-Varianten) meist automatisch eine hohe Komplexität des Regelwerks der Firewall und es müssen gegebenenfalls viele Kommunikationskanäle in der Firewall geöffnet werden.

Als ergänzende Maßnahme wäre also ein System wünschenswert, das an solchen offenen Kommunikationskanälen zielgerichtet Angriffe erkennen und im besten Fall sogar abwehren kann.

2. Intrusion Detection und Intrusion Prevention

Zum Schutz von Computersystemen vor Angriffen (Intrusions) existieren verschiedene Ansätze, die sich in ihrer Funktionalität und in ihrer Positionierung innerhalb des Computernetzwerks grundlegend unterscheiden.

Die reine Erkennung, Signalisierung und Protokollierung von Angriffen wird von den so genannten Intrusion-Detection-Systemen (IDS) geleistet, die als Ergänzung zur Firewall schon seit längerer Zeit eine Rolle spielen. IDS arbeiten ähnlich einer Alarmanlage, sie erkennen Angriffe, ver-

hindern sie jedoch nicht. Die an zentraler Stelle auflaufenden Alarmmeldungen können dabei in unterschiedliche Alarmstufen kategorisiert werden: vom einfachen Protokolleintrag über eine E-Mail-Benachrichtigung bis hin zur automatisch generierten SMS an den Systemadministrator. Die sich daran anschließende Maßnahme unterliegt allerdings einer Reaktionszeit im Minuten- oder Stundenbereich und erlaubt somit im Wesentlichen die Analyse der Vorgehensweise des Angreifers, um Maßnahmen gegen zukünftige Attacken der gleichen Form ergreifen zu können.

An dieser Stelle greift das Konzept der Intrusion-Prevention-Systeme (IPS). Ein IPS besteht im Prinzip aus zwei Komponenten: Eine Komponente leistet (analog zu einem IDS) auf Basis eines dedizierten Regelwerks die Analyse des Netzverkehrs und die Erkennung verdächtiger Kommunikationsmuster. Die zweite Komponente führt dann automatisch Gegenmaßnahmen durch, die Einbrüche in das System bzw. schadenstiftendes Verhalten unterbindet.

Abhängig von der Positionierung eines IDS bzw. IPS unterscheidet man Netzwerk-basierte und Host-basierte Systeme. Letztere werden auf einem Host installiert und schützen im Sinne einer „Last Line of Defense“ insbesondere diesen vor Angriffen bzw. dessen Folgen, verhindern aber auch die Ausbreitung eines Angriffs über

die Schnittstelle zum Netz. Ein Netzwerk-basiertes System wird als zusätzliche Komponente in das Netzwerk integriert. Es wird dabei meist transparent (d.h. als Bridge) in einen zu überwachenden Link eingebracht und fungiert als Filter. Pakete, die zu einer als schädlich erkannten Kommunikationsbeziehung gehören, werden verworfen. Andernfalls werden die Pakete weitergeleitet. Für diesen IPS-Typ hat sich auch der Begriff Inline IPS eingebürgert. Der Vorteil liegt hierbei nicht allein in dem umfassenderen Schutz, sondern auch in der Konzentration der Ressourcenanforderungen auf separate Systeme, so dass Performance-Einbußen durch eine IDS-/IPS-Applikation auf Seiten der Endgeräte vermieden werden. Dem gegenüber bietet die Host-basierte Installation den Vorteil der Erkennbarkeit von Angriffen, die über verschlüsselten Netzverkehr erfolgen, sowie einer direkten Nachvollziehbarkeit eines Angriffs. Bei hoher Netzlast besteht bei Netzwerk-basierten Systemen die Gefahr, dass sie zum Engpass bei der Datenübertragung werden. Die Folge wäre entweder eine niedrigere maximale Übertragungsrate oder eine geringere Schutzwirkung, da nur ein Teil der Pakete untersucht werden kann.

Tabelle 1 zeigt eine Übersicht der verschiedenen Lösungsansätze.

Gemeinsam ist allen Systemen, dass durch ein gewisses Regelwerk versucht

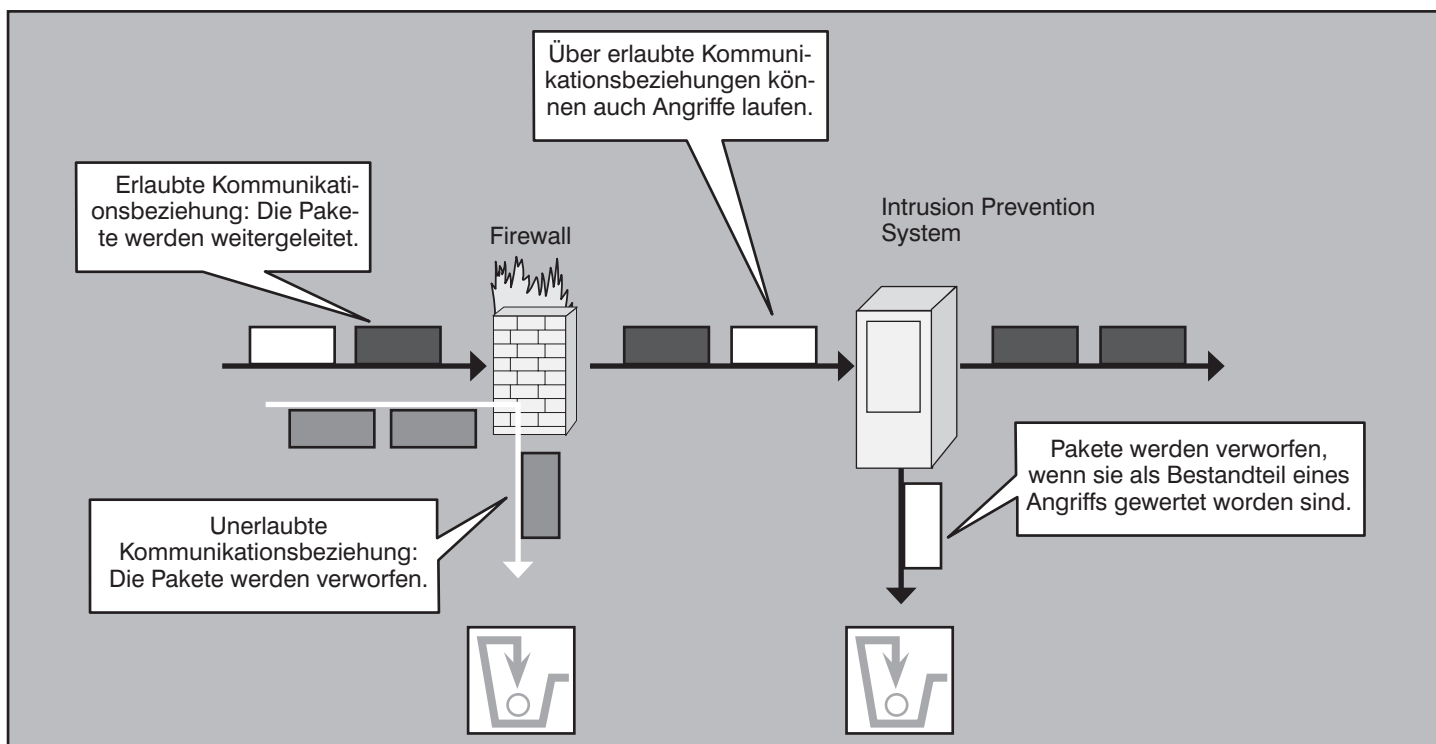


Abbildung 1: Paketfilter im Zusammenspiel mit einem Intrusion Prevention System

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

	Bedeutung	Implementierung	Funktion	Positionierung
NIDS	Netzwerk-basiertes Intrusion-Detection-System	Appliance	Erkennung von Angriffen	Netzwerk inline
HIDS	Host-basiertes Intrusion-Detection-System	Software	Erkennung von Angriffen	Host
NIPS	Netzwerk-basiertes Intrusion-Prevention-System	Appliance	Aktive Abwehr von Angriffen	Netzwerk inline
HIPS	Host-basiertes Intrusion-Prevention-System	Software	Aktive Abwehr von Angriffen	Host

Tabelle 1: Übersicht der verschiedenen Lösungsansätze zur Abwehr von Angriffen

wird, Anomalien in der Kommunikation zu erkennen. Damit ergibt sich zwangsläufig ein Problem in der Feinjustierung der Regeln. Sind die Regeln zu schwach formuliert, bleiben schadenstiftende Datenpakete unentdeckt oder führen zu keiner Abwehrmaßnahme bzw. zu keinem Alarm („False Negatives“). Sind die Regeln hingegen zu restriktiv definiert, können auch Pakete verworfen werden (bzw. zu einem Fehlalarm in einem IDS führen), die eigentlich keinen problematischen Hintergrund haben („False Positives“).

Die Wichtigkeit eines sorgfältig entworfenen Regelsatzes wird an folgendem Beispiel deutlich: Angenommen, ein IPS verfügt über eine Regel, die bei erkannten Port Scans sowohl eingehende als auch ausgehende Kommunikation mit der dazugehörigen IP-Adresse verhindert bzw. verwirft. Nun hat aber ein Angreifer seine IP-Adresse nur vorgetäuscht (IP Spoofing) und dabei die Adresse eines für das angegriffene Computersystem wichtigen Update-Servers verwendet. Fortan werden also sämtliche Update-Versuche durch das IPS unterbunden.

3. Funktionsweise eines IPS

Bei einem Host-basierten IPS (HIPS) handelt es sich um einen Software-Agenten, der auf einem Host einen Schutzmantel um den Betriebssystemkern bildet. Dies geschieht, indem der Agent den Zugriff auf Betriebssystemressourcen kontrolliert und auf Anomalien hin untersucht. Dazu gehören beispielsweise der schreibende Zugriff auf Systembibliotheken, die Speicherzuweisung für Applikationen und der wechselseitige Zugriff von Applikationen auf Elemente des Betriebssystems. Da hierbei eine Analyse der Aktionen und Auswirkungen bei einem Angriff auf das System erfolgt, kann ein HIPS auch ohne detaillierte Kenntnisse des Angriffsschemas auf eine

Attacke schließen und bietet daher einen gewissen Schutz bei unbekannten Angriffen, so genannten Day-Zero-Attacken.

Auch bei Netzwerk-basierten IPS (NIPS) gibt es verschiedene Erkennungsmethoden, um Angriffe auf das Computersystem zu verhindern (siehe Abbildung 2). Protokollanomalien, d.h. Abweichungen zu einer Spezifikation, können erkannt werden und zur Blockierung von Datenpaketen führen. Dies beinhaltet auch die Erkennung von bewusst fehlerhaften Parametern, wie sie zur Erzeugung eines Buffer Overflows genutzt werden. Hierfür analysiert das NIPS die Abfolge der Datenpakete, um eine Abweichung von der Norm des betreffenden Protokolls aufzuspüren und eine Entscheidung über die weitere Vorgehensweise (Weiterleitung oder Blockierung) zu treffen.

Aber auch Anomalien des Paketverlaufs können auf einen Angriff hindeuten, wie

z.B. DoS- oder DDoS-Attacken. Zur erfolgreichen Erkennung derartiger Abweichungen muss anhand einer statistischen Erhebung über Art und Umfang des Datenverkehrs zunächst eine geeignete Norm (Baseline) definiert werden. Hierfür analysiert und protokolliert das NIPS den Netzwerkverkehr. Beispielsweise können Pakete, die zwischen zwei Adressen ausgetauscht werden, hinsichtlich der am häufigsten auftretenden Adresse bzw. des häufigsten Adressbereichs oder hinsichtlich des prozentualen Anteils unterschiedlicher Protokolle am Gesamtnetzverkehr analysiert werden. Aus diesen Informationen wird eine Baseline generiert. Angriffe werden als von dieser Baseline stark abweichende Netzaktivität erkannt und können den entsprechenden Paketen zugeordnet werden, die das NIPS daraufhin verwirft.

Als Schutzmaßnahme auf Applikationsebene kommt darüber hinaus eine signaturbasierte Angriffsabwehr zum Einsatz. Dabei werden die Paketinhalte des Datenstroms auf Pattern untersucht, die einem bekannten Angriffsschema entsprechen und in einer Signatur abgespeichert wurden. Hier können z.B. E-Mails auf verdächtige Inhalte bzw. Dateianhänge untersucht werden. Eine zusätzliche kontextsensitive Berücksichtigung des Status einer Verbindung oder die Kopplung mit der Suche nach Protokollanomalien kann hinsichtlich Effektivität und Effizienz der Angriffserkennung deutliche Vorteile erzielen.

Die Erkennungsregeln eines IPS müssen analog zum klassischen Virenschutz bei Bedarf, d.h. bei neuen Signaturen oder neuen Verhaltensmustern, aktualisiert werden. Das Regelwerk ist dabei Bestand-

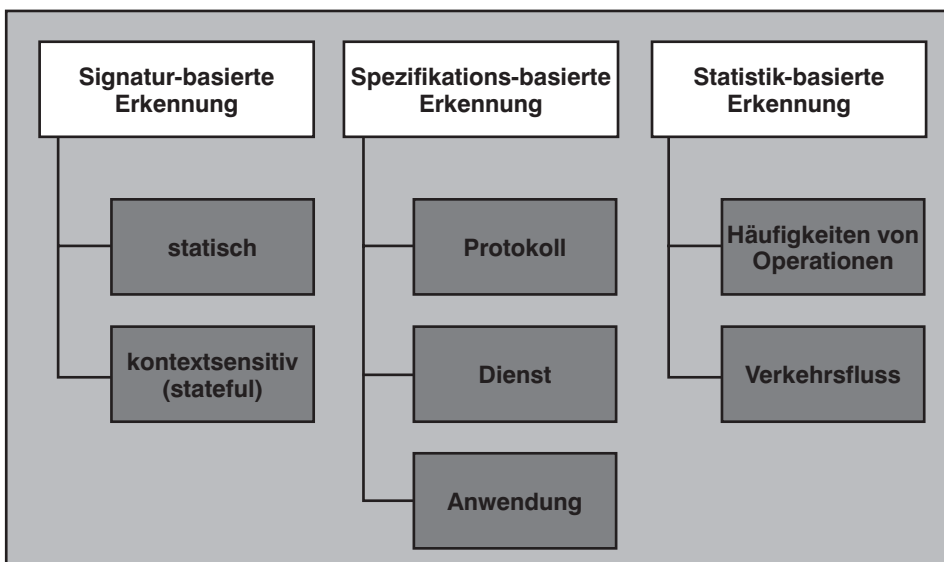


Abbildung 2: Methoden zur Anomalie-Erkennung durch ein Netzwerk-basiertes IPS

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

teil des Produkts und muss nicht notwendigerweise vom Nutzer selbst spezifiziert werden. Der Nutzer gestaltet typischerweise lediglich die Auswahl der Regeln.

Die Mechanismen, die der signaturbasierten Angriffsabwehr zu Grunde liegen, werden im Folgenden anhand des Open Source IPS Snort-Inline beschrieben (siehe [5] und [6]).

Als Beispiel dient dabei die Erkennung eines Wurms, der sich z.B. über ein Peer-to-Peer-Netz ausbreitet, sowie dem Verhindern seiner weiteren Ausbreitung über das interne Netz. Die Signatur einer solchen - sich in Binärform ausbreitenden - schadenstiftenden Software, sollte aus mindestens 32 Hexadezimalwerten bestehen, die einen charakteristischen Ausschnitt der Binärcodierung des Wurms darstellen. Breitet sich der Wurm in Form eines E-Mail-Anhangs aus und liegt insofern MIME kodiert vor, sollte die Signatur aus mindestens 72 Zeichen bestehen, um eine zuverlässige Erkennung zu ermöglichen und False-Positives zu vermeiden.

Die Regel, die zum Schutz vor einem Wurm-Angriff dient, hat im Fall von Snort-Inline das Aussehen wie in Abbildung 3 dargestellt.

Dabei haben die einzelnen Elemente dieser Regel die folgende Bedeutung:

- **drop tcp**
weist Snort-Inline an, ein TCP-Paket zu verwerfen, wenn es die im Folgenden definierten Eigenschaften aufweist. Neben den ebenfalls unterstützten Protokollen UDP und ICMP, können darüber hinaus weitere Protokolle ergänzt werden.
- **\$EXTERNAL_NET any -> \$HOME_NET any**
bezeichnet die Adressen, Portnummern und die Richtung der beobachteten Kommunikation. Dabei stellen **\$EXTERNAL_NET** und **\$HOME_NET** die entsprechenden Platzhalter für das fremde und eigene Netz dar. Auf welchen Portnummern die Pakete eintreffen, spielt in diesem Fall keine Rolle (any), die Überwachung beschränkt sich jedoch auf den eingehenden Datenverkehr. Soll die Kommunikation in beiden Richtungen überwacht werden, ist die Verknüpfung der IP-Adressen durch **<>** zu ersetzen.
- **msg:"W32/Vessier.worm.a - SMB"**
definiert die Meldung, die auf der Konsole ausgegeben oder in die Protokoll-datei bzw. Datenbank geschrieben wer-

```
drop tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"W32/Vessier.worm.a - SMB";
content: „|7B 5A 51 56 B0 30 AC F5 34 3B 06 C8 7A 4E 64 44 A5 EC 91 47 53 58
EA|“; classtype: incoming-worm-traffic; rev 1;)
```

Abbildung 3: Beispiel einer Regel für Snort-Inline

den soll. An dieser Stelle ist auch eine Anweisung an externe Programme zur Signalisierung per SMS o.ä. denkbar.

- **content: „|7B 5A 51 ... 53 58 EA|“**
spezifiziert die Signatur, deren Auftreten innerhalb des Datenstroms aufgespürt werden soll. Hexadezimale Werte werden bei Snort neben den Anführungszeichen zusätzlich mittels des Pipe-Symbols (|) einschachtelt.
- **classtype: incoming-worm-traffic**
bietet während der Protokollierung die Möglichkeit zur Kategorisierung von Angriffen. Anhand einer zentralen Konfigurationsdatei können dabei seitens des Benutzers beliebige Klassentypen definiert werden.
- **rev 1**
ermöglicht aus Gründen der Übersichtlichkeit die Vergabe einer Versionsnummer für jede erstellte Regel.

Um die Präzision der Angriffserkennung zu verbessern, können mehrere Inhalte (content) gleichzeitig abgefragt oder das zu erkennende Muster mittels einer PCRE

(PERL Compatible Regular Expression) beschrieben werden. Dies ermöglicht bei sorgfältiger Formulierung des regulären Ausdrucks insbesondere die Detektion von neuen Angriffen, für die noch keine explizite Regel existiert, die aber ein gegenüber früheren Angriffen ähnliches Schema aufweisen (Day-Zero-Angriffe).

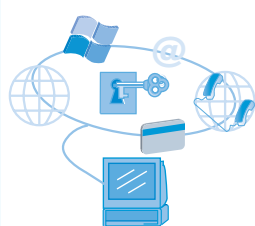
Snort-Inline ist eine Weiterentwicklung vom ursprünglich reinen IDS Snort zu einem Intrusion-Prevention-System. Die Bezeichnung „inline“ weist dabei darauf hin, dass sich diese Version von Snort zwischen den Netzwerkverkehr schaltet, um mittels des Kommandos drop Pakete verwerfen und damit Angriffe aktiv abwehren zu können.

4. Einsatzszenarien für ein Netzwerk-basiertes IPS

Der Einsatz eines NIPS ist in allen Bereichen der IT-Infrastruktur denkbar, in denen Sicherheitsbereiche getrennt und potentiell Angriffe abgewehrt werden müssen (siehe Abbildung 4):

- Außenanbindung: Ein NIPS kann als ergänzende Maßnahme zu einer Firewall

IT-SECURITY KONGRESS



IT-Sicherheits-Forum 2006 08.05. - 11.05.06 in Bad Neuenahr

Das Programm dieses hochaktuellen Sicherheits-Kongresses besteht aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen. Das Forum verbindet die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Am 3. Tag werden in parallelen Sessions stark praxisorientierte Workshops durchgeführt. Dazu gehören moderierte Produktvergleiche (u.a. zu Content Security Gateways, Application Firewalls) ebenso wie die gemeinsame Erarbeitung von Lösungsszenarien (u.a. für Notfallkonzepte, Sicherung kritischer Infrastrukturen, sichere Adminumgebungen).

Moderation: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

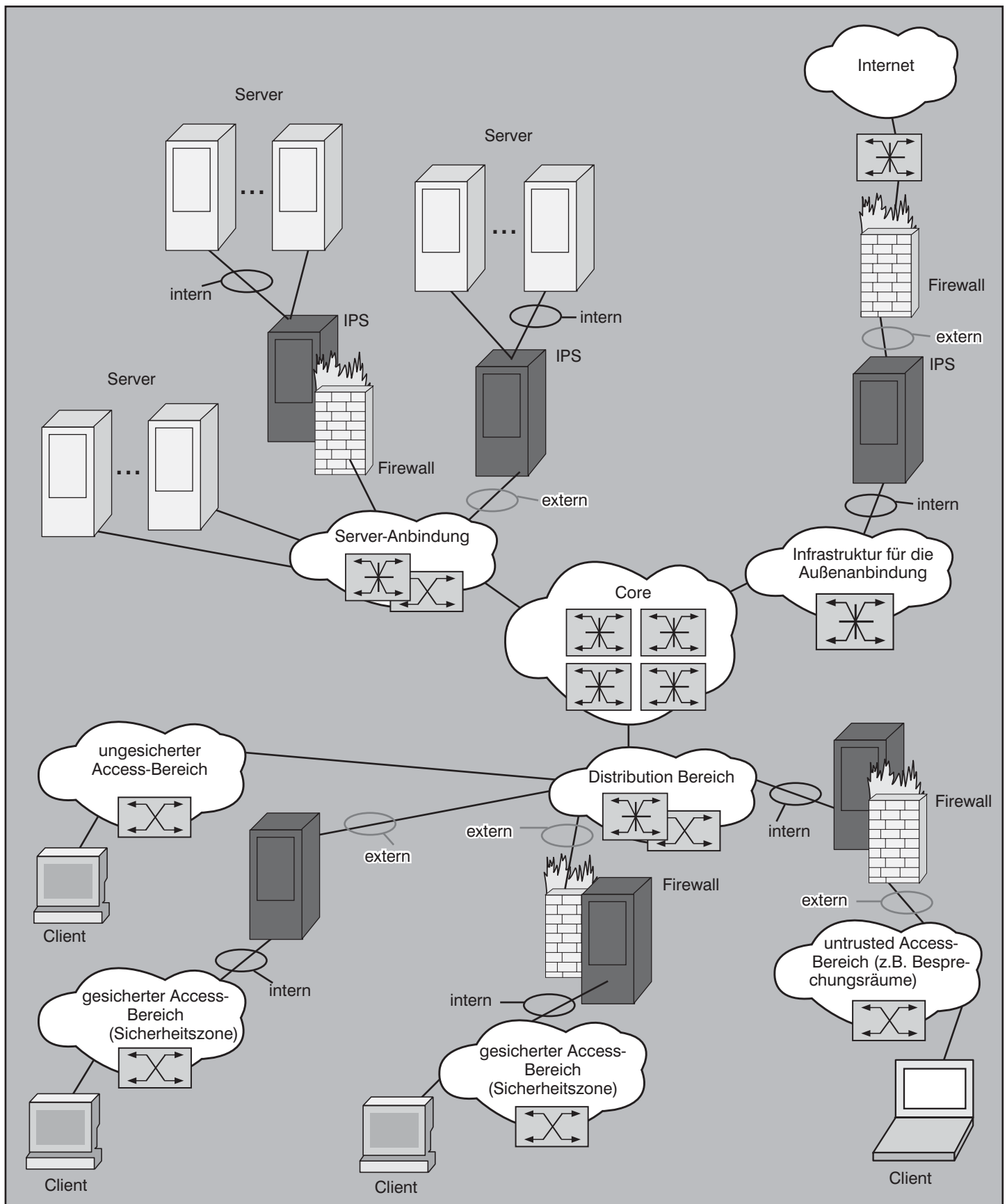


Abbildung 4: Beispiele für den Einsatz eines NIPS

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

zur Absicherung von Zugriffen auf Server in einer DMZ und für Zugriffe über VPN auf LAN-Ressourcen (d.h. vom VPN-Gateway zum internen LAN hin) dienen.

- **Serveranbindung:** Server mit einem hohen bis sehr hohen Schutzbedarf, insbesondere Server, die aus technischen Gründen nicht adäquat gepatcht werden können, lassen sich mit einem NIPS schützen. Auf Server-Ebene kann grundsätzlich natürlich auch ein HIPS eingesetzt werden. Vorteil eines NIPS ist hier, dass die Schutzmaßnahme keinen Eingriff auf den Servern selbst erfordert.
- **Endgerätenanbindung:** Mit einem NIPS können Sicherheitsbereiche abgetrennt werden, in denen Endgeräte mit einem entsprechend hohen Schutzbedarf gruppiert und durch ein NIPS (oft in Kombination mit einer Firewall) vor Angriffen und unberechtigten Zugriffen geschützt werden. Beispielsweise können in einem solchen Sicherheitsbereich Geräte abgesichert werden, die nicht gepatcht werden können bzw. die außerhalb der Kontrolle der IT liegen (z.B. PCs in Maschinen).

Im Server- und Endgerätebereich ist der ausschließliche Einsatz von Firewalls

manchmal schwierig, da die Regelwerke entweder sehr komplex sein müssen, um die vielfältigen erlaubten Kommunikationsbeziehungen zu überwachen, oder sie sind aus einer Sicherheitsperspektive zu grobmaschig. Der Vorteil eines NIPS ist an dieser Stelle, dass es weitgehend unabhängig von den genutzten Anwendungen konfiguriert werden kann.

Der Einsatz eines NIPS innerhalb des LAN auf der Ebene der Server- und Endgerätenanbindung erfordert vom NIPS eine hohe Durchsatzleistung. Weiterhin hat ein NIPS generell einen Einfluss auf die Latenzzeit (Übertragungszeit) von Paketen und deren Varianz (Jitter). Daher muss für Dienste und Anwendungen, die Anforderungen an die Latenzzeit haben bzw. empfindlich gegenüber Jitter sind (z.B. VoIP), die Veränderung der Latenzzeit durch ein NIPS genau geprüft werden.

Zur Sicherstellung einer hohen Verfügbarkeit ist in vielen Fällen der redundante Aufbau eines NIPS erforderlich. Typischerweise operiert ein NIPS als Inline IPS auf Layer 2 und ist für Redundanzmechanismen auf Layer 3 (z.B. OSPF und VRRP) in der Regel transparent. Es ist daher meist unproblematisch ein redundantes IPS-Paar in ein hochverfügbares Netzwerk-Design zu integrieren (siehe Abbildung 5), und es ist nicht erforderlich an der Netz-

werkkonfiguration (speziell an der Layer-3 Konfiguration) Änderungen vorzunehmen.

Damit im Fehlerfall bei einem Wechsel von einem IPS auf ein anderes IPS bestehende Sessions nicht unterbrochen werden, ist es notwendig, dass zwischen den IPS Zustandsinformationen (State Synchronization) ausgetauscht werden. Dies wird von einigen Herstellern (z.B. Tipping Point) unterstützt.

5. Marktsituation

Am Markt ist inzwischen eine recht zufriedenstellende Palette an kommerziellen, Netzwerk-basierten IPS verfügbar. Teilweise sind die Hersteller auf Intrusion-Prevention-Systeme spezialisiert, wie etwa Tipping Point oder Top Layer Networks, und manche Hersteller kommen wie im Fall von McAfee aus dem Virenschutzbereich. Auch klassische Anbieter von Netzwerkkomponenten, wie Enterasys, Cisco und Juniper Networks, haben ihre Produktpalette um Sicherheitslösungen erweitert, zu denen auch IPS gehören. Neben Firewalls und VPN-Lösungen bieten Sonicwall und Fortinet auch Netzwerk-basierte Intrusion-Prevention-Systeme an. Dabei liefert Fortinets FortiGate ein Beispiel für die Kombination von Firewall- und IPS-Funktionalität. Dass der Firewall-Hersteller Check Point Software den Snort-Entwickler Sourcefire übernimmt, sei hier nur am Rande erwähnt.

Interessant ist in diesem Zusammenhang die Feststellung, dass es nicht nur kombinierte Firewall-IPS-Systeme gibt: Zur gezielten Abwehr von sich über das Netzwerk ausbreitenden Viren, Würmern und Trojanern existiert von Trend Micro eine Lösung, die im weitesten Sinne eine Mischung eines Virenschutzsystems mit IPS-Konzepten darstellt. Die in unterschiedlichen Ausbaustufen erhältlichen „VirusWalls“ werden im Netzwerk direkt vor besonders zu schützenden Endgeräten positioniert. Dort analysieren sie den Datenstrom einerseits signaturbasiert, andererseits anhand statistischer Erhebungen, um bei Auffälligkeiten schadenstiftende Datenpakete entfernen und die weitere Ausbreitung des Virus im Netz verhindern zu können.

Mit Lucid Security, SecurityMetrics und VarySys wird der Markt mit kleineren Herstellern erweitert, die anstelle einer eigenen Entwicklung eine IPS-Appliance auf Basis von Linux und dem bereits angesprochenen Snort-Inline anbieten.

Was die Leistungsfähigkeit der am Markt befindlichen Geräte angeht, steht ein breites Produktspektrum mit Bandbreiten zwischen 250 MBit/s und 3 GBit/s sowie einer

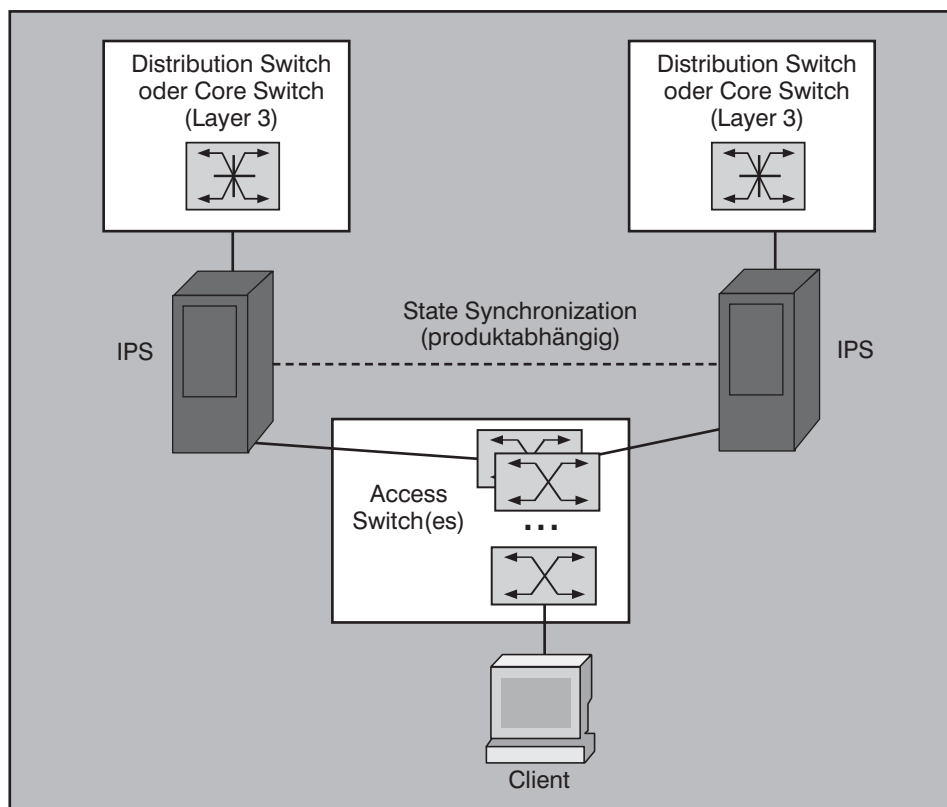


Abbildung 5: Aufbau eines redundanten IPS-Paars

Zwischen Firewall und Virenschutz: Intrusion-Prevention-Systeme

unterschiedlichen Zahl von Netzwerk-Ports (teilweise in optischer Ausführung) zur Verfügung.

Bei manchen Geräten kann die Verfügbarkeit durch redundante Netzteile erhöht werden. Um die Netzkommunikation auch im Notfall aufrecht erhalten zu können, können sich die Geräte mancher Hersteller (z.B. Tipping Point) bei Auftreten eines Fehlers oder bei einem kompletten Ausfall als reine Layer-2-Switches verhalten. Diese Funktion ist allerdings kritisch zu bewerten, da hier die Kommunikationsverfügbarkeit über den Schutz vor Malware gestellt wird.

Das Management kann in Abhängigkeit des jeweiligen Herstellers über eine separate Anwendung, ein Command-Line-Interface oder eine Web-basierte Oberfläche vorgenommen werden, so dass auch hier eine komfortable Integration in Computernetze unterschiedlicher Größe möglich ist.

6. Zusammenfassung und Ausblick

IPS haben sich in ihren verschiedenen Varianten (Host-basiertes IPS und Netz-basiertes IPS) als Bestandteil des „Werkzeugkastens“ der IT-Sicherheit etabliert und ergänzen dabei Firewalls und Systeme für den Virenschutz. Ein IPS ist dabei streng genommen ein spezieller Filter, der sich im Gegensatz zu einer klassischen Firewall weniger für erlaubte Kommunikationsbeziehungen, sondern mehr auf Abweichungen und Anomalien konzentriert. Netz-basierte IPS ergänzen dabei nicht nur die Perimetersicherheit, sondern insbesondere auch die Sicherheit innerhalb des LAN, indem mit ihnen Sicherheitszonen geschaffen werden können. Firewalls und IPS werden nicht unberührt nebeneinander existieren. Es zeichnet sich ab, dass vermehrt beide Funktionen in einem Netzelement integriert werden. Vereinfachend formuliert wird dem Paketfilter eine zusätzliche Entscheidungslogik zugefügt. Für den Nutzer ergibt sich neben dem einheitlichen Management der Vorteil der Vereinfachung des Netzdesigns.

7. Literatur

Neben der folgenden Aufstellung weiterführender Literatur zum Thema Intrusion-Prevention befinden sich zusätzliche Informationen auf den Webseiten der genannten Hersteller.

- [1] Spennberg, Ralf, „Intrusion Detection and Prevention mit Snort 2 & Co“, Addison-Wesley, 2004.

- [2] Northcutt, Stephen, Novak, Judy, „Network Intrusion Detection“, Hüthig Telekommunikation, 2004.

- [3] Becker, Frank, Petermann, Matthias, „Intrusion Detection Systems Elevated to the Next Level“. 22nd Chaos Communication Congress, Dezember 2005, http://events.ccc.de/congress/2005/fahrplan/attachments/560-Paper_IntrusionDetectionSystems.pdf

- [4] Eine reichhaltige Sammlung an Literatur und Links zum Thema IDS und IPS findet sich unter <http://www.honeypots.net/ids/links>

- [5] <http://www.snort.org>

- [6] <http://snort-inline.sourceforge.net>

HIDS	Hostbased Intrusion Detection System
HIPS	Hostbased Intrusion Prevention System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
NIDS	Networkbased Intrusion Detection System
NIPS	Networkbased Intrusion Prevention System
OSPF	Open Shortest Path First
PCRE	PERL Compatible Regular Expression
PERL	Practical Extraction and Report Language
RPC	Remote Procedure Call
SMS	Short Message Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
RRRP	Virtual Router Redundancy Protocol

8. Abkürzungen

DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DoS	Denial of Service

IT-SECURITY KONGRESS



IT-Sicherheits-Forum 2006

08.05. - 11.05.06
in Bad Neuenahr

Gemeinsame Veranstalter des IT-Sicherheits-Forums sind die ComConsult Akademie und die GAI NetConsult Berlin. Dieser einzigartige Security-Kongress, der von Dipl.-Inform. Detlef Weidenhammer, Geschäftsführer der GAI NetConsult, geleitet wird, zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat einen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier aller Erfahrung nach immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

Moderation: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

Neuerscheinung März 2006

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.

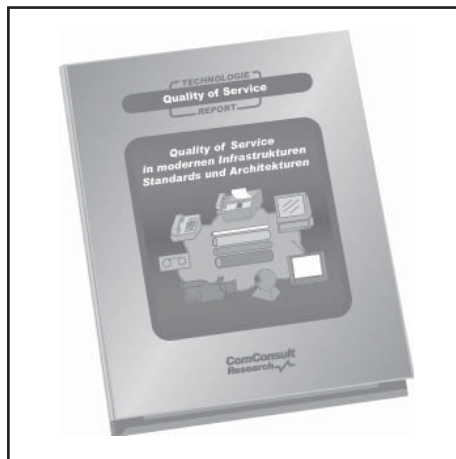
Im Folgenden stellen wir Ihnen einen Auszug als Leseprobe zur Verfügung:

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.

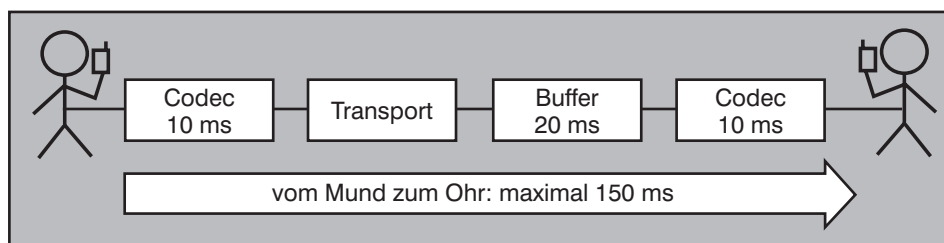


Abbildung 1: Delay-Annahmen

Quality of Service in modernen Infrastrukturen

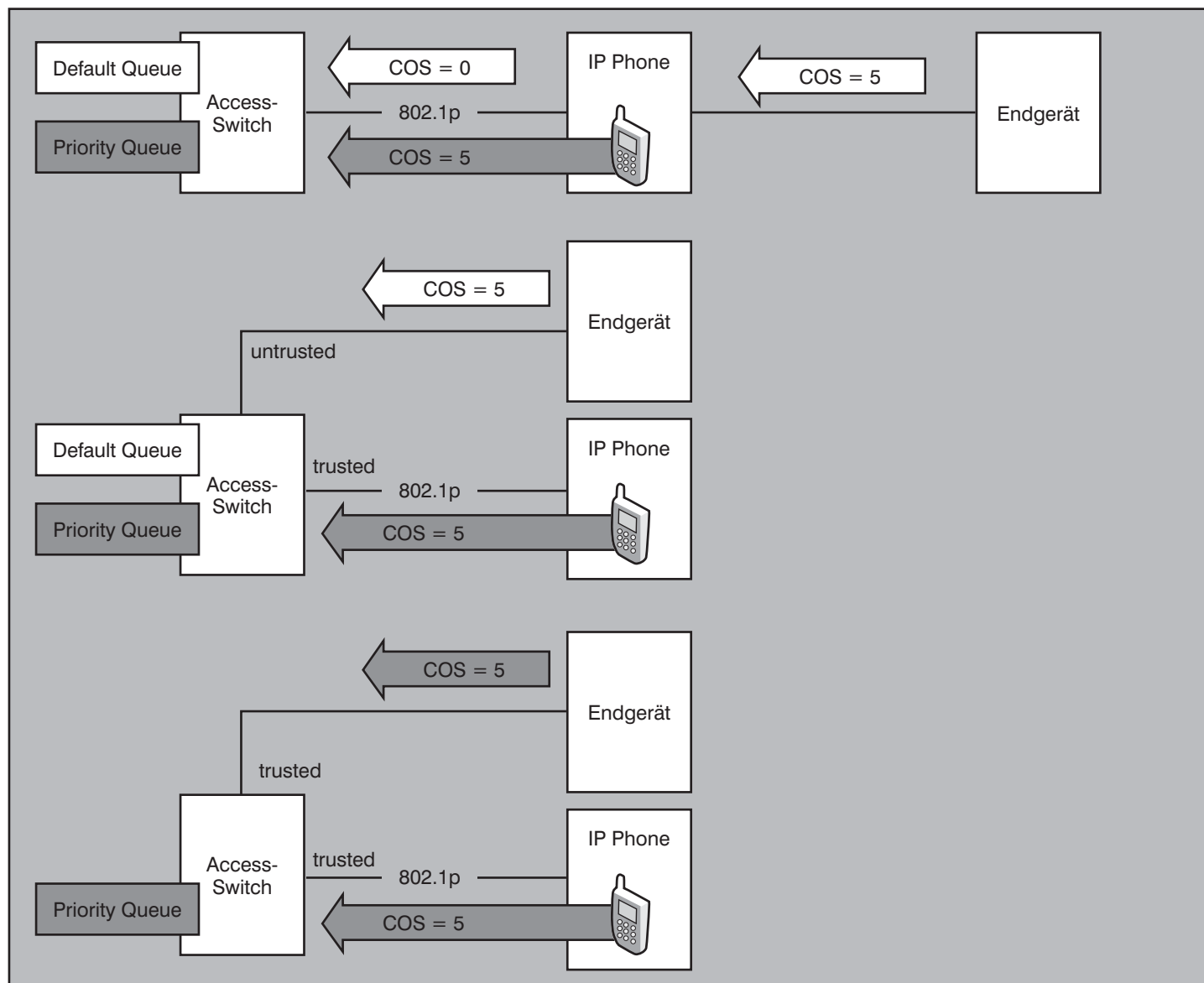


Abbildung 2: Priorisierung gemäß IEEE 802.1D/p

Fax-Antwort an ComConsult 02408/955-399

Bestellung Quality of Service

☐ Ich bestelle den Report
Quality of Service
in modernen Infrastrukturen
(Preis € 398.-- zzgl. MwSt. und Versand)

Die Studie wird ab Mitte März ausgeliefert.

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

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift

Sicherheitsmechanismen für Voice over IP

Die ComConsult Akademie veranstaltet vom 17. - 18. Mai erstmalig ihr neues Seminar „Sicherheitsmechanismen für Voice over IP“ in Bonn.

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.

In diesem Seminar wird vermittelt,

- was sich in Bezug auf Informationssicherheit mit der Umstellung auf VoIP ändert,
- welche Gefahrenpotenziale berücksichtigt werden müssen,
- welche Standards für VoIP-Sicherheit relevant sind,
- wie die Vertraulichkeit der Sprachkommunikation in IP-Netzen geschützt werden kann,
- worauf beim Design von VoIP-Umgebungen hinsichtlich Verfügbarkeit zu achten ist,



- wie die IP-Telefonie in vorhandene Sicherheitsstrukturen in Netzen einzubinden ist,
- welche Probleme bei VoIP über Vertrauensgrenzen hinweg entstehen und wie sie zu lösen sind,
- welche rechtlichen Aspekte bei VoIP-Sicherheit relevant sind.

Der Referent Dr. Frank Imhoff blickt auf jahrelange Projekterfahrung im Bereich VoIP und Informationssicherheit zurück und vermittelt diese Erfahrungen im Seminar.

Zum Inhalt

- Unterschiede zwischen konventioneller Telekommunikation und VoIP hinsichtlich Sicherheit
- Bekannte und denkbare Angriffsszenarien
- Standards für VoIP-Sicherheit
- Verschlüsselung von VoIP
- Design hochverfügbarer VoIP-Umgebungen
- IP-Telefonie vor dem Hintergrund von Netzwerksicherheitsmechanismen
- VoIP über Vertrauensgrenzen hinweg
- VoIP-Sicherheit aus der Sicht der Gesetzgebung und Regulierung
- Sicherheitsarchitektur für zwei VoIP-Anwendungsszenarien
- ComConsult-VoIP-Security-Standard

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sicherheitsmechanismen für Voice over IP

- ☐ Ich buche das Seminar
Sicherheitsmechanismen für Voice over IP

vom 17. - 18.05.06 in Bonn
zum Preis von € 1.390,- zzgl. MwSt.

- ☐ Bitte reservieren Sie für mich
ein Hotelzimmer

vom _____ bis _____ 06

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort



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

eMail

Unterschrift

Aktuelle Veranstaltungen

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 20.03. - 24.03.06 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.

Design von Voice-Ready Netzen und WLAN Integration, 20.03. - 22.03.06 in Bad Neuenahr

Dieses Seminar vermittelt dem Fortgeschrittenen in 3 Intensiv-Tagen, mit welchen Varianten und Alternativen ein modernes Netzwerkdesign erreicht werden kann, das den Herausforderungen Konvergenz, Mobilität und Sicherheit gewachsen ist wie unter Nutzung der neuesten Redundanz- und Switching-Verfahren ein LAN optimal gestaltet werden kann und wie dabei die Anforderungen von Client-, Server- und Speicher-Systemen im Sinne von Verfügbarkeit, Verkehrs- und Betriebsoptimierung architektonisch integriert werden können.

Preis: € 2.490,- zzgl. MwSt.

Trouble Shooting in konvergenten Netzwerken, 27.03. - 31.03.06 in Aachen

Dieses Seminar vermittelt das notwendige Hintergrundwissen über die typischen Fehler, erklärt ihre Erscheinungsformen im laufenden Betrieb und trainiert systematisch ihre Diagnose und Beseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Preis: € 2.490,- zzgl. MwSt.

Lokale Netze für Einsteiger, 03.04. - 07.04.06 in Düsseldorf

Dieses 5-tägige Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert.

Preis: € 2.290,- zzgl. MwSt.

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clients, WLANs, 03.04. - 07.04.06 in Aachen

Dieses 5-tägige Seminar vermittelt intensiv den praktischen Umgang mit Firewall, VPN, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt.

Preis: € 2.290,- zzgl. MwSt.

Planung und Betrieb mobiler Kommunikation, 04.04. - 05.04.06 in Zürich-Glattbrugg

Dieses Seminar analysiert die beim Betrieb von mobilen Teilnehmern und Geräten zu lösenden Aufgaben und gibt Empfehlungen zur optimalen Umsetzung. Auch die typischen Fallstricke werden benannt. Auf der Basis von vielen Beispielen wird die geeignete Handhabung der verschiedenen Technikbereiche erklärt. Dabei zeigt sich, dass Mobilität als Kernanforderung für konvergente Netze einen maßgeblichen Einfluss auf Architektur und Betrieb hat.

Preis: € 1.390,- zzgl. MwSt. (CH: € 1.490,-)

Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen, 04.04. - 05.04.06 in Zürich-Glattbrugg

Sie erfahren in diesem 2-tägigen Seminar, welche typischen Ursachen den in den letzten Jahren festgestellten Störungen und Schäden in Netzwerken und DV-Installationen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können.

Preis: € 1.390,- zzgl. MwSt. (CH: € 1.490,-)

Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung basierend auf dem Cisco-Call-Manager in einem großen Netzwerk, 04.04. - 05.04.06 in Zürich-Glattbrugg

Dieses 2-tägige Seminar beschreibt eine Telefonie-Komplettlösung auf Basis des Cisco-Call Managers ergänzt um CTI-, UMS- und IVR-Funktionen. In einem Unternehmensnetz mit über 100 Standorten und 30.000 Arbeitsplätzen werden bereits über 40 vernetzte CallManager-Cluster und weit mehr als 10.000 IP-Telefone zentral administriert und betrieben. In dem Mix aus Erfahrungsberichten, der Darstellung von Verfahren, technischen Hintergründen, Beispielen zu Systemkonfigurationen und eigenen Entwicklungen betrachten die Referenten, die selbst Betreiber der Lösung sind, die wichtigsten Facetten des Projektes.

Preis: € 1.390,- zzgl. MwSt. (CH: € 1.490,-)

IP-Telefonie evaluieren, planen, betreiben, 24.04. - 26.04.06 Jolly Hotel in Köln

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

Preis: € 1.690,- zzgl. MwSt.

Trouble Shooting für TCP/IP- und Windows-Umgebungen, 24.04. - 28.04.06 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen in diesem Umfeld, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Preis: € 2.490,- zzgl. MwSt.

Netzwerk Design 2006: Anforderungen, neue Technolo- gien, Trends - Teil 2

Fortsetzung von Seite 1



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

Die Vision der Wireless Mesh Hersteller ist eine grundlegende Änderung des WLAN Marktes, unter ihnen sind sowohl etablierte als auch Start Up Namen zu finden: Accton, BelAir Networks, Cisco / Airespace, D-Link (in 2006), FireTide Networks, InterDigital Communications, Motorola / MeshNetworks, NextHop Technologies (Client Adapter), Nortel, PacketHop, Strix Systems, Thomson, Tropos Networks, TrueMesh (Client Adapter). Laut Dell'Oro wird der Mesh WLAN Markt in 2007 auf ein Volumen von 2 Mrd. USD anwachsen.

5.1 Zielsetzung und Übersicht

Im Gegensatz zu ihrem Namen erfordern drahtlose LAN's (WLANs) heute noch eine erkleckliche Menge an drahtgebundenen Anschlüssen, nämlich für jeden einzelnen Access Point mindestens einen Ethernet-Anschluss, bei redundanter Anbindung auch an zwei Ethernet-Anschlüsse. In Gebäuden mit existierenden Verkabelungssystemen und fixer Infrastruktur stellt dies ein geringeres Problem dar. Aber was ist bei ad-hoc Netzen bei ebenso kurzfristigen wie vorübergehenden Vernetzungen wie Medien-Events oder Katastrophenfälle? Eine Zielsetzung vermaschter WLANs ist es daher, den Verkabelungsbedarf so weit wie möglich zu minimieren und die Flexibilität in Form von Mobilität und ad-hoc Einrichtung mobiler Netzwerke damit so weit wie möglich zu maximieren. Dies wird über eine Vernetzung der Access Points mittels Funkverbindungen anstelle der Ethernet-Ankopplung(en) erreicht.

Einfach auf den Punkt gebracht, nutzen vermaschte WLANs eine Topologie mit vermaschten Funkverbindungen zwischen den einzelnen Knoten, um ein selbstkonfigurierendes, fehlertolerantes d.h. „selbstheilendes“ Netzwerk zu bilden. Da nur einige wenige vermaschte Knoten mit einer

Kabel-Anbindung (Ethernet) ausgestattet werden, entfällt einerseits der Bedarf für aufwändige Backbone-Verkabelungen, andererseits werden die Vorteile von optimierter Routenfindung, Lastverteilung und automatischer Fehlerumschaltung auf alternative / Backup Wege erreicht, die zentrale Management-Kontrolle bleibt als Vorteil erhalten (siehe Abbildung 5.1). Hierbei können zentrale Controller als Steuerinstanz zum Einsatz kommen, dies muss jedoch nicht immer der Fall sein; einige Architekturen bestehen auch aus einem reinen „Peer-Netzwerk“ intelligenter vermaschter Knoten, die gleichberechtigt untereinander Informationen austauschen.

Vorteile von Mesh WLANs sind:

- bessere Skalierbarkeit
- automatische Skalierbarkeit

- schnelles Handover
- Schnelle Implementierbarkeit
- Minimierung der benötigten Verkabelungs-Infrastruktur

Die IEEE 802.11 Standardisierung arbeitet mit IEEE 802.11s ebenfalls an einer vermaschten Lösung. Hier steht allerdings erst etwa Mai 2006 ein Anfangs-Konsens auf dem Terminplan, nachdem im Juli 2005 15 verschiedene Vorschläge eingereicht wurden (5 vollständige Vorschläge, 10 Vorschläge mit partieller Abdeckung). Ein stabiler Draft bzw. verabschiedeter Standard ist für etwa Anfang bis Mitte 2007 zu erwarten. Der Standard wird Bezug nehmen auf QoS nach IEEE 802.11e / WMM und Sicherheit nach IEEE 802.11i / WPA.

Um die Verabschiedung von IEEE 802.11s erstens zu beschleunigen und zweitens mit einem gewissen Marktgewicht zu beeinflussen, hat sich die Wi-Mesh Allianz (WMA) gebildet, die einen gemeinsamen Erstvorschlag bei der IEEE 802.11s Arbeitsgruppe eingereicht hat. Mitglieder der WMA sind z.B. Accton, InterDigital, Mitre, NextHop, Nortel, Philips, Swisscom Innovations und Thomson.

Der WMA-Vorschlag ist eine Spezifikation, die den vollständigen IEEE 802.11s Funktionsumfang umfasst und enthält insbesondere

- Unterstützung für Einzel- und Mehrfach-Antennen (Singel / Multi-Radio)
- Verkehrs-Kontrolle an den verteilten Knoten durch Erweiterung von IEEE 802.11e auf vermaschte Strukturen
- Selbstkonfigurierung der Knoten mittels standalone Modus oder in Verbindung mit einem Infrastruktur Netz (z.B. BSS)
- Dynamisches Routing mit Nutzung alternativer MAC Datenpfade für Unicast, Multicast und Broadcast
- Unterstützung verschiedener Routing Verfahren auf der Basis von MAC-Adressen und Hello Paketen (für Discovery und Assoziierung von WLAN „Maschen“)
- Authentifizierung und Schlüsselmanagement für den Austausch von Routing Informationen sowohl in zentralisierten als auch in verteilten Vermaschungs-Modellen
- Sicherheit, insbesondere Unicast-/Multicast-Verschlüsselung über mehrere Hops hinweg, unabhängig von den eingesetzten Radio-Typen; sichere Assoziierung benachbarter Knoten bei Ablauf der Beacon oder Hello Timer; Hop-by-Hop Authentifizierung, auch für Multicast und Tunneling

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

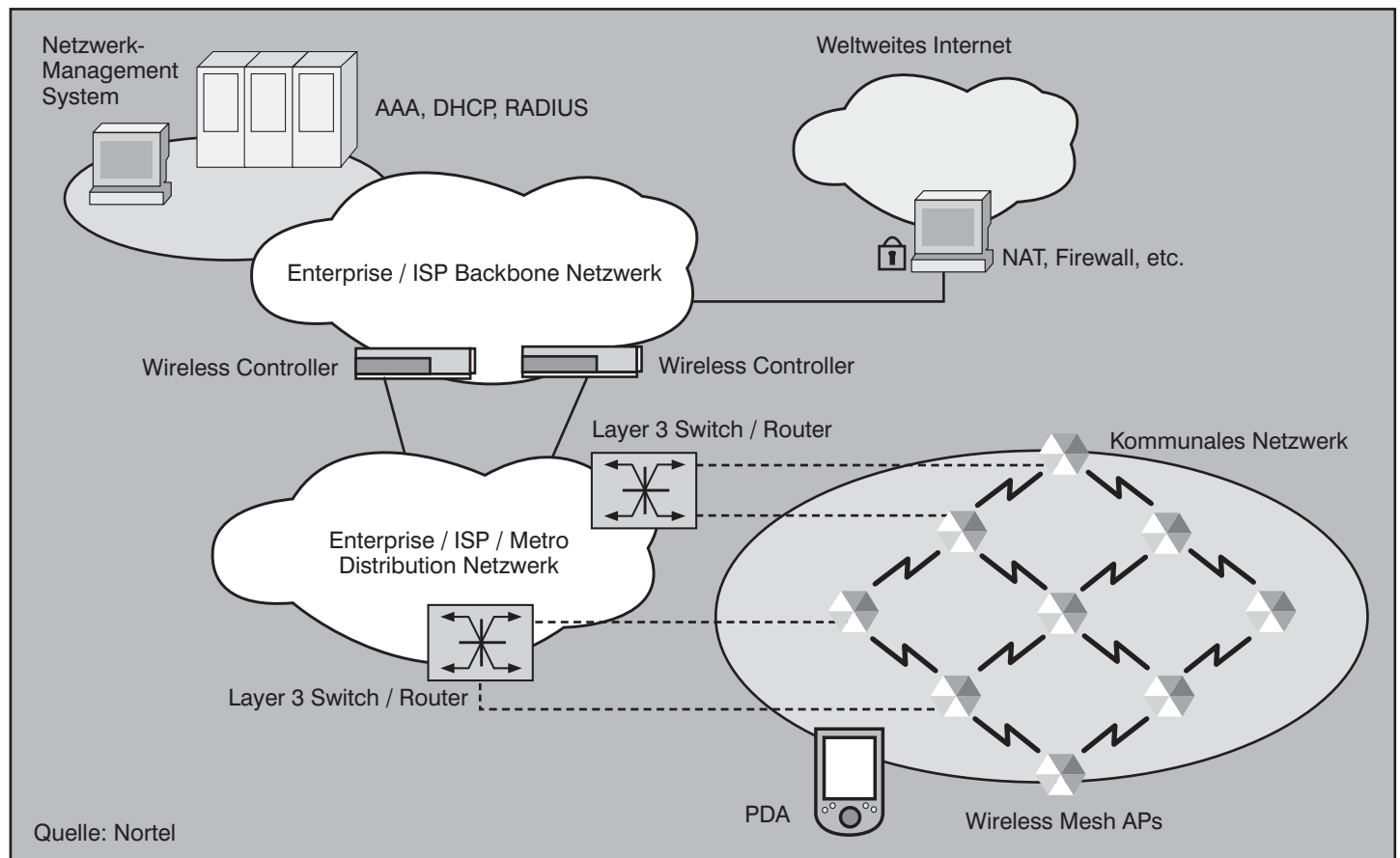


Abbildung 5.1: Mesh WLAN Gesamtszenario mit Ankopplung an Ethernet / IP Backbones und zentralem Management

Eine Übersicht der verschiedenen Funktionsmodule, die die WMA in ihrem Vorschlag für eine vermaschte Architektur nutzt und / oder neu definiert, ist in Abbildung 5.2 gezeigt. Die Schnittstelle „nach oben“ zu anderen vermaschten WLANs oder zu einem Wireline Backbone bildet das Modul „Mesh Interworking“. Darunter liegen Messungen, Routing und Sicherheits-Funktionsmodule, die jedoch noch oberhalb des MAC Sublayer angesiedelt sind. Zum MAC Sublayer gehört eine Koordinierung der Vermaschung (MCF, Mesh Coordination Function), die die bekannten Zugriffs-Kontrollfunktionen HCCA und EDCA überlagert. Ergänzt wurde als weitergehende Reservierung der Distributed Reservation Channel Access (DRCA). Mesh WLANs sollen mit allen verabschiedeten MAC Standards (11a/b/g/h/j) zusammen funktionieren.

Die Mesh Coordination Function (MCF) beschreibt z.B. folgende Funktionen:

- Koordinierung des Kanalzugangs über mehrere Knoten hinweg, d.h.: über mehrere Hops hinweg Leistungs-Einbrüche zu vermeiden und / oder QoS Anforderungen erfüllen; Peer-to-Peer

Kommunikation über eine vermaschte Struktur unterstützen; verteilte Auto-konfiguration der vermaschten WLAN Komponenten ermöglichen

- QoS Aspekte wie: Priorisierung bestimmter Verkehrslasten innerhalb eines vermaschten WLANs, Flußkontrolle über mehrere Hops hinweg, Unterstüt-

zung eines Verfahrens zur Handhabung konkurrierender Zugriffe (Contention Resolution) und Kontrolle der Multicast- und Broadcast-Verkehrslast innerhalb eines vermaschten WLANs

- Power Save Unterstützung (Frame-Bearbeitung unter Berücksichtigung des Power Budgets)

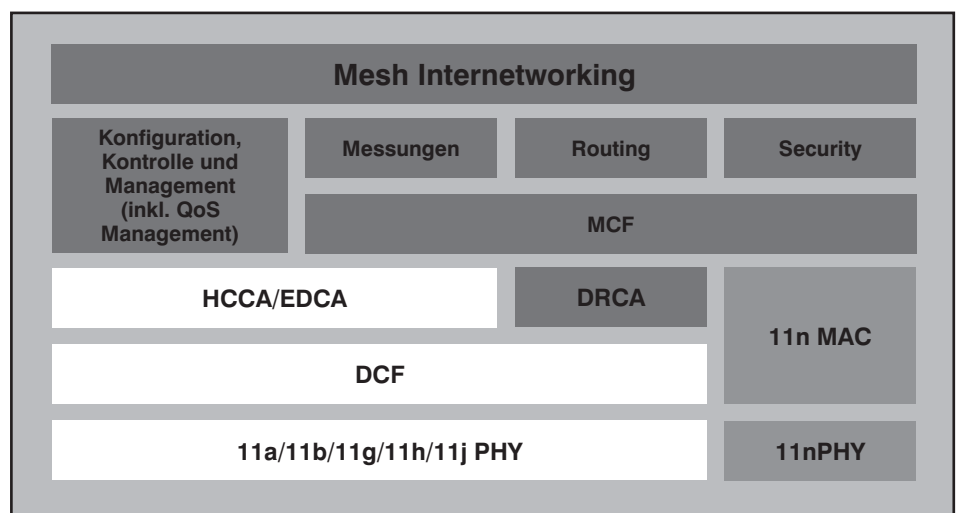


Abbildung 5.2: Mesh WLAN Architektur des WMA-Vorschlags

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

- Effiziente Verwaltung der RF Frequenzen und räumlichen Verteilung, z.B. Vermeidung von Leistungseinbußen durch versteckte oder abgelegene Knoten, Unterstützung mehrerer parallel aktiver Antennen zur Kapazitäts-Erweiterung

5.2 Vermaschte WLANs: Funktionsweise und Architektur-Typen

Ein vermaschtes WLAN bildet eine Backbone-Struktur auf der Basis von Funkverbindungen auf. Dieser vermaschte WLAN Backbone könnte auch als Funkzellen-Cluster beschrieben werden. So genannte Backbone Access Points (AP's) oder WLAN Router nutzen mehrere aktive Funkverbindungen (mindestens eine eingehende und eine ausgehende) zum Informationsaustausch und zur Weiterleitung von Daten, konfigurieren sich selbst (über diese Funkverbindungen), finden andere, benachbarte AP's und wählen für die Weiterleitung von Daten den günstigsten Weg auf der Basis von Echtzeit RF-Bedingungen aus. Eine Erweiterung des vermaschten WLANs geschieht durch Einschalten eines weiteren Access Points. Dieser fügt sich automatisch in das vermaschte WLAN ein, erhöht die Kapazität und / oder stellt weitere Alternativ-Wege zur Verfügung. Kurz gesagt - die Knoten eines vermaschten WLANs verhalten sich ähnlich wie Layer-3 Switches und Router eines verkabelten LANs.

Die Anbindung eines vermaschten WLANs an verkabelte Backbone-Netze erfolgt über wenige (optional redundante) Backbone-AP's, die zusätzlich zu den Funkschnittstellen auch noch über Ethernet-Schnittstellen verfügen. Teilweise werden diese in Herstellerlösungen Network Access Points (NAP) genannt (z.B. Nortel), teilweise werden sie als WLAN Router oder WLAN Gateway bezeichnet.

Typische Einsatzbereiche vermaschter WLANs sind

- Ad-Hoc Netzwerke
- (Medien-)Events
- Baustellen
- Messen
- Notfall-Szenarien (Hurrikan, Flutkatastrophe, Erdbeben, ...), die bei zerstörter Verkabelungs-Infrastruktur ad-hoc Netze für Polizei, Feuerwehr, Notärzte, Katastrophenschutz, THW etc. erfordern.

Endgeräte / Clientsysteme sind im Regelfall ebenfalls über WLAN assoziiert, in einigen Fällen sind Client oder Front End AP's verfügbar, die die Clientsysteme über mehrere geschaltete Ethernet-Schnittstellen anschalten (Front-End Ethernet, z.B. FireTide). In diesem Fall ist der Front-End AP ein Ethernet-Miniswitch mit 4 bis 8 Ethernet-Schnittstellen 10/100Base-TX und ein bis mehreren Backbone-Funkverbindungen über IEEE 802.11a/b/h/g (oder auch WiMAX!). Die von den Clients erwartete

oder verarbeitbare Eingangs-Last findet ihre Limitierung somit nicht in der Summe der Ethernet-Schnittstellen sondern in der Summe der Funkschnittstellen. Ein Einsatz-Szenario mit Backbone AP's, Transit AP's sowie Front End / Client AP's mit und ohne Ethernet Schnittstellen ist in Abbildung 5.3 dargestellt.

Wesentliche Funktionselemente eines vermaschten WLANs sind zu:

- Nutzung der lizenzfreien Frequenzbänder (IEEE 802.11)
- Unterstützung von Indoor und Outdoor-Komponenten
- Autodiscovery
- Dynamisches Routing mit Fehlerumschaltung („Self-Healing“) und Wegeoptimierung (Best Path)
- Optional: QoS für Unicast und Multicast
- Fast Handoff
- Load Balancing
- Funk-Eingangs-Schnittstelle (Mesh Ingress) und Funk-Ausgangs-Schnittstelle (Mesh Egress) an einem Knoten / Client
- Optional Ethernet Eingangs- und Ausgangs-Schnittstellen an einem Knoten
- Client Dienst (soweit Clients nicht Mesh Knoten sind)
- Automatische Erweiterbarkeit (Autokonfiguration)
- Unterstützung von Einfach-Antennen (Single Radio) und Mehrfach-Antennen (Multiple Radio)
- Sicherheit: Erweiterung von IEEE

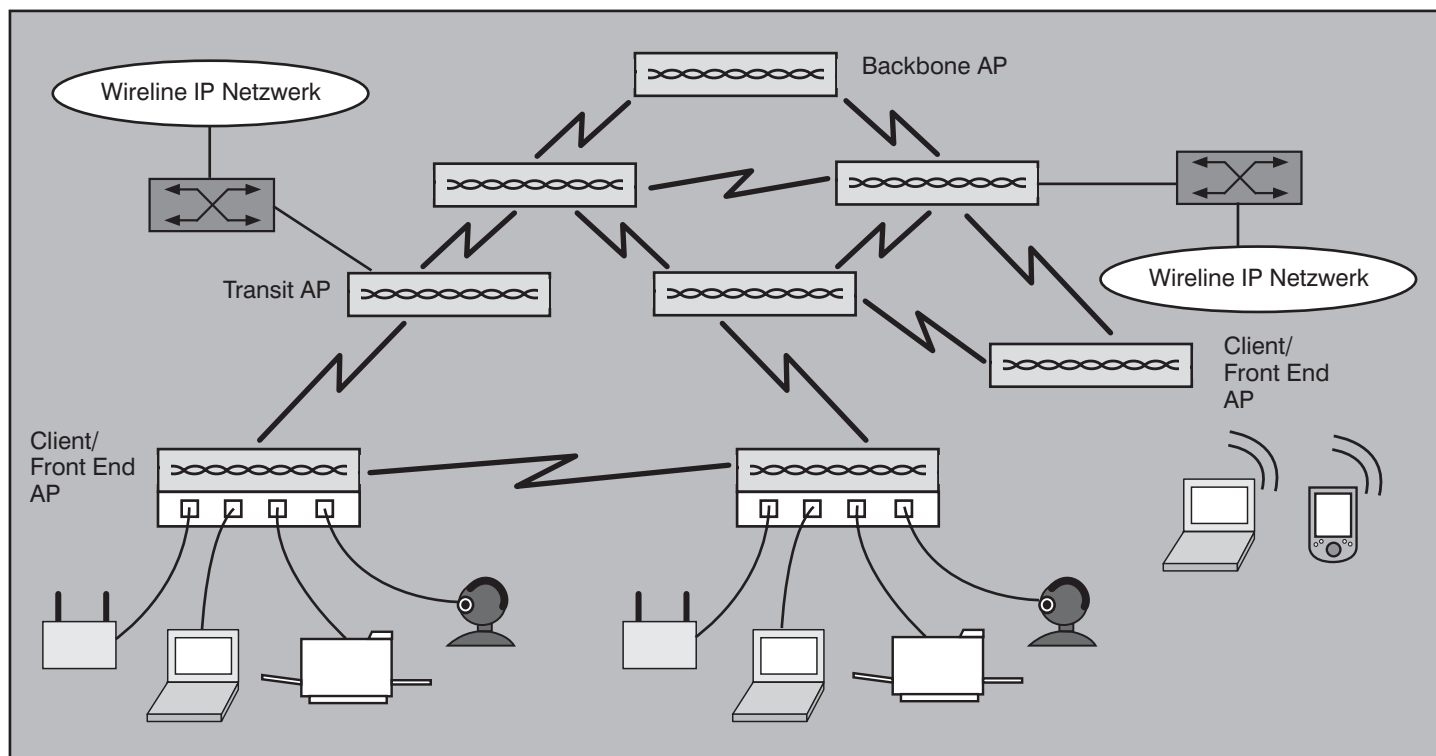


Abbildung 5.3: Mesh WLAN Einsatzszenario

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

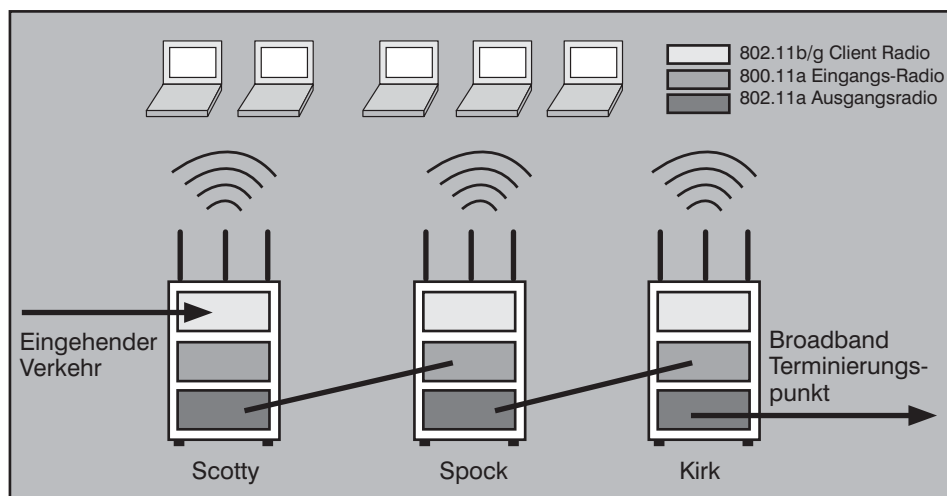


Abbildung 5.4: Frame-Weiterleitung im vermaschten WLAN

802.11i auf vermaschte Topologien: Authentifizierung der Knoten

- Optional: Autorisierung, Verschlüsselung

Ein sehr einfaches Einsatz-Szenario zeigt Abbildung 5.4, das gezeigte Beispiel enthält eine WLAN-Kaskade mit 3 Hops. Knoten Scotty empfängt auf seinem Eingangs-Interface (Ingress) die Daten aller angebundenen bzw. assoziierten WLAN-Clientsysteme oder auch Ethernet-Clientsysteme (!). Er leitet sie intern auf sein WLAN Ausgangs-Interface weiter (Egress), bei einer Einzel-Antenne ist dies dasselbe Interface wie der Ingress, auf dem die Daten empfangen wurden. Zur Verbesserung der Antwortzeit kann die Weiterleitung erfolgen, bevor alle eingehenden Pakete eines Sendeslots zu Ende empfangen wurden. Die Egress Antenne leitet die Frames zum nächsten Nachbarn weiter, wobei der verwendete Routing-Algorithmus diesen Nachbarn wegetechnisch optimiert hat; im gezeigten Beispiel ist dies Knoten Spock. Die Ingress-Antenne von Spock empfängt den gesamten Verkehr von Scotty's Egress Antenne, also Routing Informationen und weitergeleitete Daten-Frames. Der so bei Spock eingehende Verkehr wird von ihm mittels interner Bearbeitung zu seinem Ausgangs-Interface „geschwicht“, von dort weitergeleitet und am Ingress Punkt von Knoten Kirk empfangen. Kirk's Transit Interface leitet den Verkehr an das angeschlossene verkabelte Backbone-Netzwerk weiter, z.B. an eine dort angeschlossene Serverfarm.

Nutzung von Mehrfach-Antennen

Die Nutzung von Mehrfach-Antennen und Antennen-Arrays (siehe Abbildung 5.5) ist sehr sinnvoll, um die erreichbare Kapazität zu erhöhen bzw. die Leistungs-De-gradierung einer Einzel-Antenne zu ver-

meiden (wie unter Punkt 5.4 „Offene Probleme und Verbesserungsbedarf bei Mesh WLANs“ näher beschrieben wird). Dabei ist zu bedenken, dass Mesh WLANs ja kein Selbstzweck sind, sondern irgendwo in diesem Szenario Clients sitzen, die für Senden und Empfangen von Nutzdaten bedient werden wollen! Daher ist der Einsatz von Mehrfach-Antennen mit einer – möglichst frei wählbaren – Unterteilung in Client-Antennen und Backbone-Antennen äußerst hilfreich. Typischerweise haben Mesh WLAN Produkte 6 oder mehr Antennen, die jeweils fest als Client-Dienst für Client-Assoziationen, als Ingress oder als Egress konfiguriert werden können, insbe-

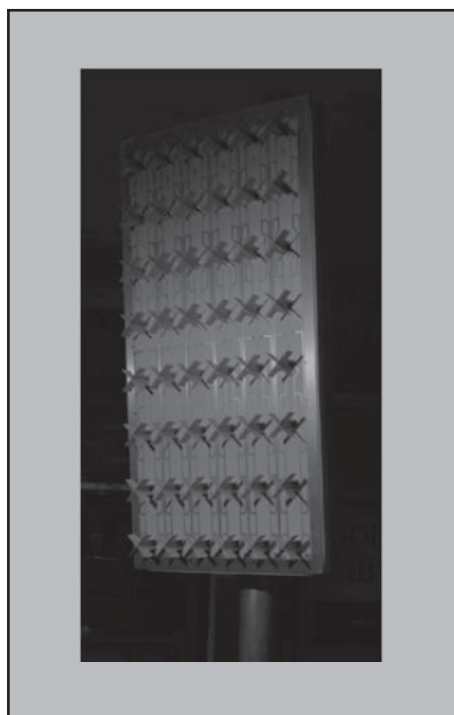


Abbildung 5.5: Antennen Array (Quelle: Nortel)

sondere für unsymmetrische Sende-/Empfangs-Lastprofile, die ja weitaus häufiger vorkommen als symmetrische Lastprofile (z.B. 3 Client-Antennen und 3 Backbone-Antennen).

Eine Ingress Antenne muss somit Assoziationen von Clients und / oder von anderen Mesh WLAN Knoten annehmen und alle damit verbundenen Daten- und Informations-Frames weiterleiten. Eine Egress Antenne muss die Verbindung zu anderen vermaschten Knoten für den Backbone-Verkehr herstellen, dabei den Ende-zu-Ende Weg optimieren und / oder als WLAN Terminierung (Broadband Termination Point) die Ankopplung an ein und Weiterleitung in ein verkabeltes Backbone-Netz leisten. Teilweise können die Client-Antennen auf dem 2,4 GHz Band und parallel die Backbone Antennen auf dem 5 GHz Band senden. Einige Produkte verwenden proprietäre, erweiterte Verfahren (z.B. QDMA von Motorola / MeshNetworks).

Der Einsatz mehrerer, im Regelfall mindestens dreier Antennen wird auch als strukturiertes Mesh WLAN bezeichnet, da die Antennen für einen bestimmten Kanal jeweils fest und mit voller Sendeleistung einer einzelnen Funktion zugeordnet sind, entweder der Client-Schnittstellen-Funktion oder der Backbone-Sendefunktion oder der Backbone-Empfangsfunktion. Auf unterschiedlichen Kanälen kann dieselbe Antenne natürlich parallel senden und empfangen. Mehrfach-Antennen können verschiedene Leistungs-Parameter innerhalb des vermaschten WLANs optimieren, darunter Kanal-Belegung, Round-Trip-Zeit, Handoff-Zeit Signalstärke und die Ende-zu-Ende Route durch das vermaschte WLAN hindurch. Somit führen vermaschte WLANs, die Komponenten mit Mehrfach-Antennen nutzen, zu einer deutlich besseren Echtzeit-Eignung als solche, in denen Komponenten mit Einfach-Antennen zum Einsatz kommen.

Mesh WLAN Typen

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

- Infrastruktur Mesh WLAN: hier sind nur WLAN Router und Access Points / Mesh Komponenten, jedoch keine Clients integriert (Hersteller z.B.: BelAir, Cisco, FireTide, Proxim, Symbol, Tropos)
- Mix Mesh WLAN: Den Kern des vermaschten WLAN Netzwerks bilden Router und Access Points mit Routing Intelligenz, Clients haben eingeschränkte

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

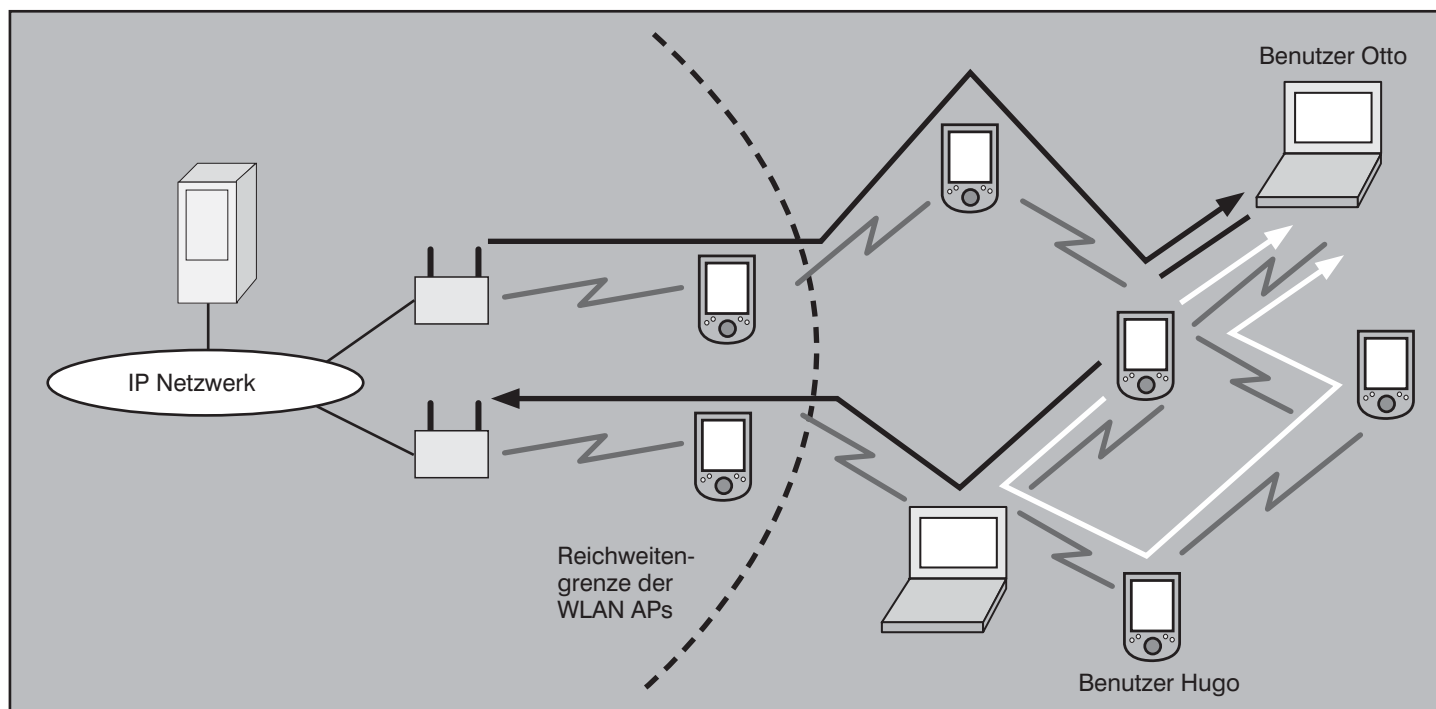


Abbildung 5.6: Client-Server Kommunikation unter Nutzung benachbarter Clients als Mesh Knoten

Routing Funktionalität (Nachbar-Erkennung, Kommunikation mit benachbarten Clients / Knoten) (Hersteller z.B.: PacketHop, MeshNetworks)

- Client Mesh: Jeder Client ist ein vollwertiger Routing Hop / vermaschter Knoten (Hersteller z.B. NextHop)

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

In einem reinen „Client Mesh WLAN“, agiert jedes (gleichzeitig mobile) Endgerät inklusive Laptops, PDA's und Softphones als Weiterleitungs-Komponente (Relay) für andere Endgeräte, d.h. die Daten eines Benutzers / Endsystems durchlaufen die aktuell benachbarten Endgeräte und „Wireless Router“ als „Hop“, um ihren Zielpartner - gegebenenfalls auch im ver-

kabelten Netzwerk - per Transit über das Funknetz hinweg zu erreichen. Die Sendeleistung beträgt z.B. 200mW, die Reichweite 500m bis 800m für IEEE 802.11b (PacketHop). Die vernetzten Clientsysteme bilden dabei ein vermaschtes Netzwerk, das automatisch „um Leistungsengpässe und Hindernisse herum“ routet. Zu beachten ist jedoch: Soweit der Routing Algorithmus auf Peer-to-Peer Kommunikation fokussiert ist, findet keine Optimierung der Client-Server Verbindungswege statt (!).

Bei Mix Mesh WLAN setzen Hersteller im Kern des vermaschten WLANs zentrale WLAN Router oder Access Points als Infrastruktur-Komponenten ein, Clientsysteme werden als eingeschränkt intelligente Mesh Knoten zur flexiblen Erweiterung des vermaschten WLANs genutzt, insbesondere hinsichtlich Ausdehnung (z.B. MeshNetworks, NextHop). Eine typische Einschränkung ist hier, dass Clients nur ihre direkte Nachbarn sehen, nicht jedoch die gesamte Topologie des vermaschten WLANs kennen, wie dies bei Mesh Routern oder Access Points der Fall ist.

Die aktive Teilnahme der Clients an der Frame-Weiterleitung („Routing“) hat auch den Vorteil, dass Handoff / Reassoziierung weggelassen, da der Client sozusagen sein eigener Router / Access Point ist. Zudem argumentieren die Hersteller von Client Mesh Netzen, dass durch die Integration der Clients als Relay-Komponenten das Problem „Reichweite vs. Abdeckung / Da-

tenrate“ entschärft wird. Client Mesh Lösungen zielen dabei mehr auf den Indoor als den Outdoor Markt.

Ein einfaches Client Mesh Szenario zeigt Abbildung 5.6. Hugo kann Daten mit Otto über zwei verschiedene Wege austauschen, wobei die Software auf Hugo's PDA hierfür die optimale Route berechnet und ausgewählt hat. Sowohl Hugo als auch Otto haben, obwohl sie sich aktuell beide außer Reichweite des nächsten Access Points bewegen, jeweils mehrere Routen durch das vermaschte WLAN hindurch zum Transit-Access Point, über den sie den Server erreichen.

Eine weitere Typisierung berücksichtigt eher den Mobilitäts-Aspekt:

- Fixed Mesh Networks: Alle Routing Hops (Knoten) haben einen festen Standort (Infrastruktur-Komponenten)
- Mobile Mesh Networks: Alle oder mehrere Routing Hops (Knoten) sind beweglich (Clients)

Routing in Mesh WLANs

Eigentlich realisieren Mesh WLANs eher ein Layer-2 Switching als ein klassisches Routing, da die Weiterleitung auf der Basis von MAC-Adressen, nicht IP Subnetzen erfolgt. Der Grund hierfür ist, dass Layer-3 Roaming vermieden werden soll, damit keine neue Authentifizierung und DHCP Konfigurierung erfolgen muss (dieses Problem ist aus nicht-vermaschten WLANs

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

hinlänglich bekannt). Dennoch wird die so genannte Multi-Hop Leistung durch Optimierung des Weges über mehrere AP's hinweg gezielt verbessert. Die Routenoptimierung heißt vielfach Best-Path Weiterleitung und erfolgt nach verschiedenen funkbhängigen und funkunabhängigen Parametern wie

- Kanalloptimierung
- Round Trip Delay
- Signalstärke (Durchsatz)
- Anzahl Hops
- Vorhandene Transitpunkte / Netzübergänge zu anderen Backbones

Ein einfaches Routing Szenario ist in Abbildung 5.7 dargestellt. Hier bilden die einzelnen WLAN Router / Access Points mit ihren jeweiligen Nachbarn ein vollvermaschtes Netz, wobei zu jedem Access Point genau eine Funkverbindung (ein Weg) aktiv ist, die anderen Funkverbindungen (Wege) befinden sich im Standby. Eine Ende-zu-Ende Verbindung wird mittels Punkt-zu-Punkt Weiterleitung umgesetzt, dies ist ein bekanntes Vorgehen aus allen (verkabelten) IP Netzwerken. Alle aktiven Verbindungen sind auf den Übergangspunkt zum Backbone Netz hin optimiert. Das dargestellte vermaschte WLAN hat eine singuläre Anbindung an ein verkabeltes Backbone-Netzwerk, die ein Single Point of Failure ist. Hier lässt sich jedoch Abhilfe schaffen, indem mehr als ein WLAN Router / Access Point an das verkabelte Backbone Netzwerk angeschlossen werden wie im Mesh WLAN aus Abbildung 5.8, das drei Knoten mit Backbone-Anbindung enthält. Dies führt zu einer lastverteilten Weiterleitung aus dem vermaschten WLAN in den verkabelten Backbone, die einer Unterteilung in drei WLAN-Bereiche mit jeweils einer eigenen Backbone-Anbindung gleichkommt, wobei der WLAN-interne aktive Weg zum Backbone-Übergang hin optimiert ist.

Im Unterschied zum Routing in verkabelten Netzen hat eine Untersuchung des MIT ergeben, dass Routing Verfahren, die eine Metrik mit Minimierung der Hopzahl nutzen oder die ausschließlich die Signalstärke optimieren, nicht in einer effizienten aktiven WLAN-Infrastruktur konvergieren. Der Grund hierfür ist einfach: Solche Routing Berechnungen korrelieren nicht mit dem tatsächlichen Durchsatz sondern erreichen weit weniger als das Durchsatz-Maximum. Dies gilt leider für alle aus der verkabelten Welt bekannten Routing Verfahren (!) und ebenso für Mesh WLAN Verfahren, die eine any-to-any Kommunikation von Peer-Clients unterstellen und die Verbindungen entsprechend optimie-

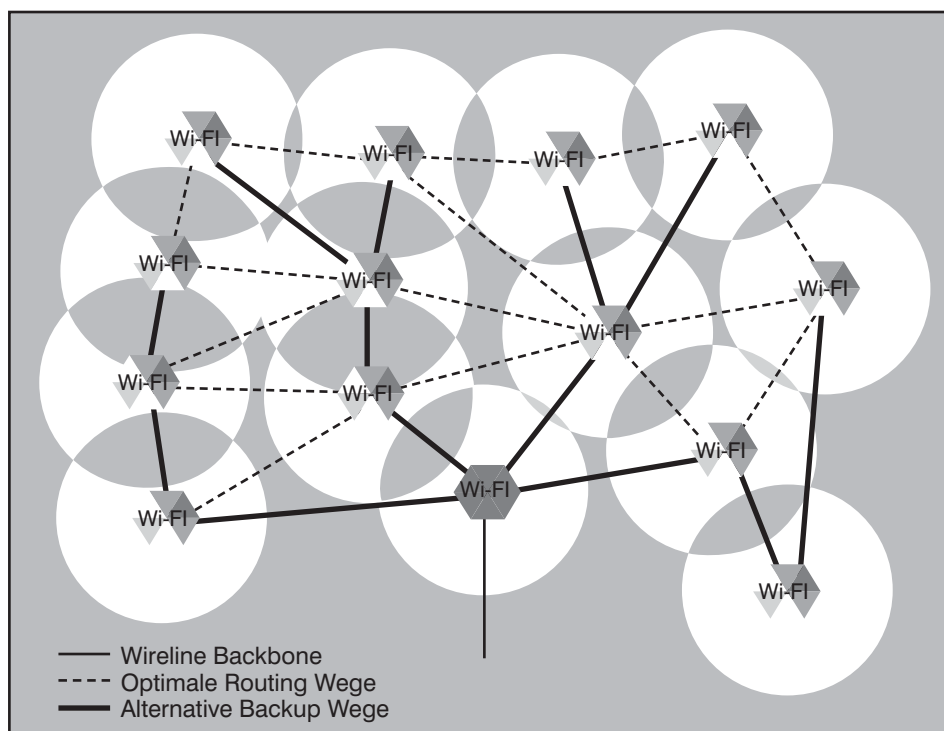


Abbildung 5.7: Vermaschtes WLAN mit aktiven und standby Verbindungen

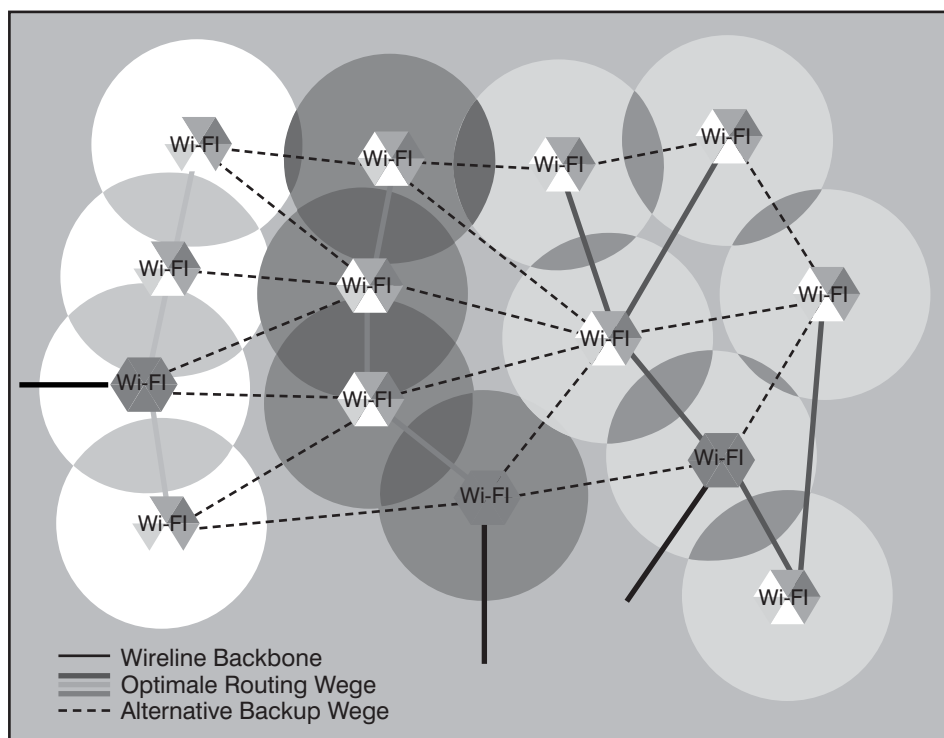


Abbildung 5.8: Vermaschtes WLAN mit Mehrfach-Anbindung an einen Backbone

ren. Zur Durchsatz-Optimierung wurden daher neue WLAN Routing Algorithmen entwickelt: Tropos führt zum Beispiel bei seinem PWRP mehrfach pro Sekunde bidirektionale Messungen durch, nutzt vorausschauende Algorithmen und wählt für eine aktuelle Weiterleitungs-Entscheidung

immer die am wenigsten ausgelasteten verfügbaren Wege aus.

WLAN Routing kann sich jedoch analog zu den klassischen Verfahren nicht nur auf Durchsatz-Optimierung beschränken, sondern soll auch automatische und zeitopti-

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

mierte Fehlerumschaltung bei Ausfall einzelner Antennen oder kompletter Access Points leisten. Hierbei ist es wichtig, dass temporäre Signalschwankungen von tatsächlichen Ausfällen unterschieden werden, da eine Routen-Neuberechnung aufgrund temporärer Schwankungen zu einem Flapping führen würde (permanenter Routenwechsel). Eine Fehlerumschaltung und Neuberechnung bei Ausfall eines Knoten, der gleichzeitig Transit-Knoten zum verkabelten Backbone ist, zeigen Abbildung 5.9 und Abbildung 5.10. Hier wird deutlich, dass die resultierende Lastverteilung nach der Fehlerumschaltung keine Gleichverteilung mehr ist, da alle Routen, die zuvor auf dem ausgefallenen Transit Knoten endeten, auf genau einen anderen Transit-Knoten umgeleitet werden.

Management von Mesh WLANs

Vielfach vertreiben die Hersteller eine spezielle Mesh-WLAN-Management-Anwendung mit einem dedizierten Management-Server, sich teilweise auf Konfiguration und Auswertungs-/Überwachungs-Statistiken beschränkt, teilweise zusätzlich Steuerungsfunktion für die vermaschten Knoten hat (Preis z.B. 10.000,- EUR bis 20.000,- EUR).

5.3 Einsatz-Beispiele für Mesh WLANs

Philadelphia

Die Stadt Philadelphia hat im Oktober 2005 einen Auftrag für ein vermaschtes WLAN für Internet Zugang mit 1 Mbit/s Datenrate über eine Fläche von 400 Quadratkilometern vergeben (Earthlink als Provider, Tropos WLAN Komponenten, Motorola Antennen) und hierfür die Erlaubnis erteilt, Antennen auf Gebäuden und Lichtmasten zu installieren. Das vermaschte WLAN soll mindestens die Hälfte der vorhandenen T1-Verbindungen ablösen.

Implementiert wird ein gesicherter WLAN Dienst für städtische Beamte im Außendienst und für öffentliche Sicherheits-Institutionen. Die Kosten eines Internet-Zugangs für Haushalte sollen maximal 20,- USD betragen, für Haushalte mit Niedrig-Einkommen 10,- USD. Die Stadt erhofft sich von dieser Maßnahme wirtschaftliches Wachstum, die Realisierung soll nach einem drei- bis sechsmonatigen Piloten über 40 Quadratkilometer noch in 2006 abgeschlossen werden.

San Francisco

In San Francisco hat das Kalifornische Amt für Notfalldienste an einem Versuch teilgenommen, bei dem mobile Mitarbeiter ad hoc Netzwerke nutzen, die insbesondere

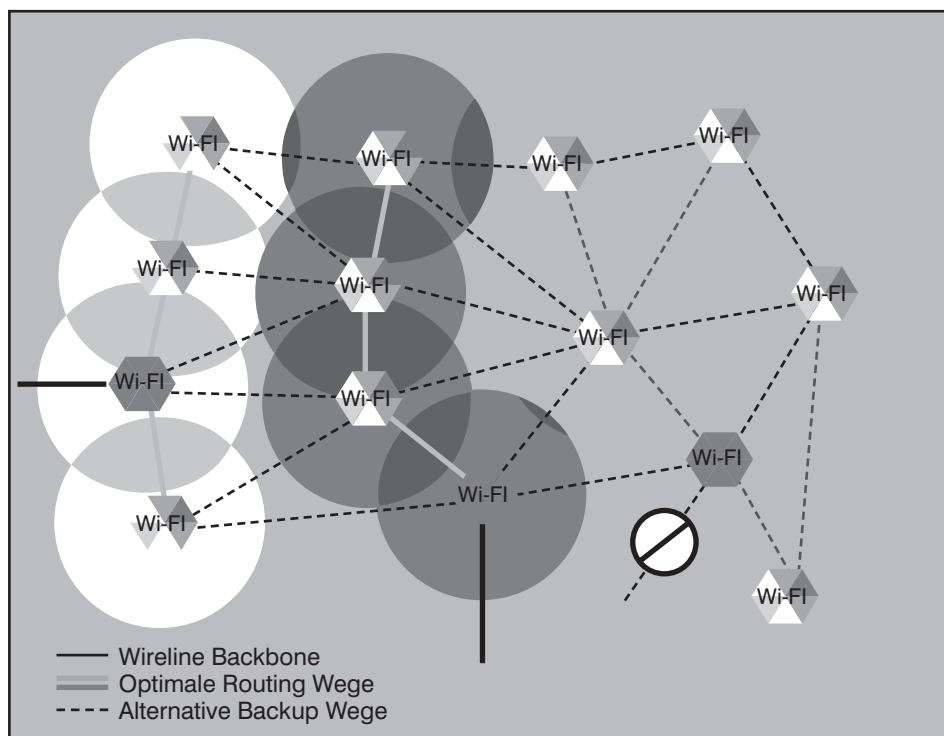


Abbildung 5.9: Ausfall eines Transit Knotens in einem vermaschten WLAN

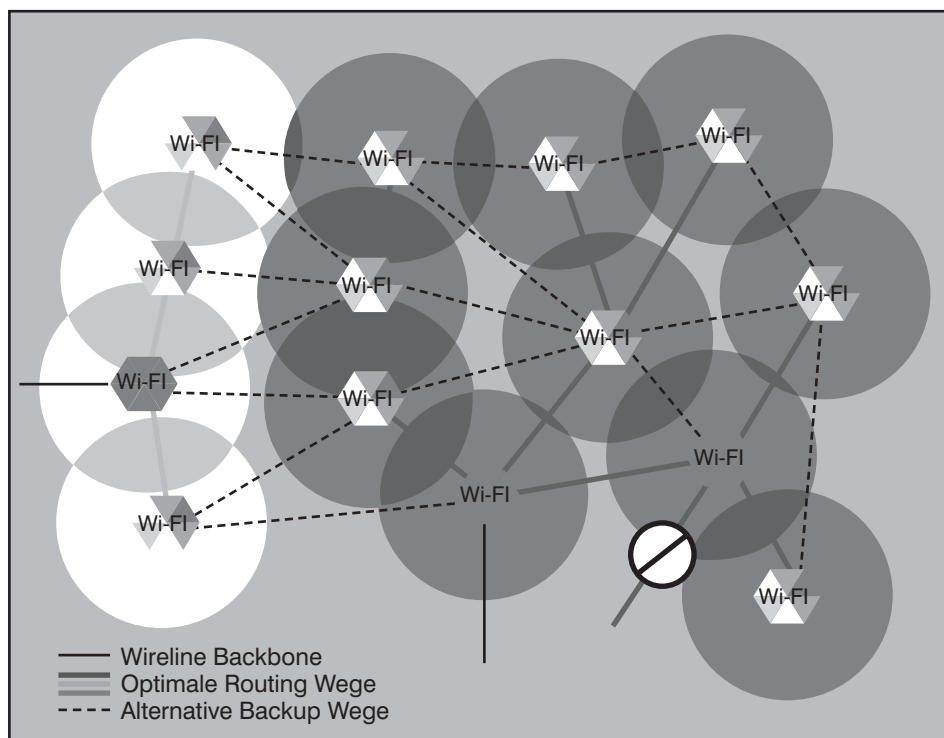


Abbildung 5.10: Aktive Wege nach dem Failover

re auch Videokamera-Überwachung implementieren (IEEE 802.11b WLAN NIC's von Proxim oder 3e Technologies Internat. mit einer Reichweite von 500 m bis 830 m, Mesh WLAN Software von PacketHop). Die Video-Auflösung ist 1/4 VGA, bis zu 30 Personen waren im Piloten gleichzeitig aktiv.

Da das vermaschte WLAN ein ad-hoc Netzwerk aus Client-Systemen waren z.B. auch Boote der Küstenwache, Polizeifahrzeuge, Feuerwehr-Fahrzeuge und mobile Leitstellen einbindbar. Die Ankopplung an einen Ethernet Backbone / RZ erfolgte über Antennenstationen auf der zentralen

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

Leitstelle. Eine Übersicht des Piloten zeigt Abbildung 5.11.

Garland und Medford

Garland (Texas) und Medford (Oregon) ersetzen einen Mobilfunk-Datendienst mit 19,2 kbit/s Datenrate durch ein vermaschtes WLAN für mobile Mitarbeiter mit 200 kbit/s bis 2 Mbit/s. Getestet wurden z.B. Peer-to-Peer Voice, Streaming Video und Stadtplan-Download von einem Polizeiserver, die Mitarbeiter befanden sich in Transporter-Fahrzeugen, die bis zu 60 mph fuhren, es sollen bis zu 100 Fahrzeuge mit WLAN Equipment ausgerüstet werden.

5.4 Offene Probleme und Verbesserungsbedarf bei Mesh WLANs

Informations-Austausch:

Ein Problem entsteht schon beim Austausch von Routing Informationen zwischen den Access Points: Jede vermaschte Funkverbindung / jeder Knoten muss für den Austausch von Routing Informationen den selben Kanal wie die jeweiligen Nachbarn nutzen (einer sendet, alle hören), auch über mehrere Hops hinweg! Nach 4 bis 5 Hops fällt dann die Leistung sehr stark ab. PacketHop gibt an, dass der genutzte (proprietäre) Routing Algorithmus den Durchsatz optimiert und der Durchsatz sich nach 4 bis 5 Hops bei 60% bis 70% des ursprünglichen Wertes stabilisiert. Hierbei wird der Durchsatz eines IEEE 802.11g NIC mit 20 Mbit/s bis 23 Mbit/s kalkuliert, so dass bei einer Kaskade von 4 bis 5 Hops noch von einem Durchsatz-Niveau von 12 Mbit/s bis 14 Mbit/s auszugehen ist.

Einzel-Antennen:

Für Access Points mit nur einer Antenne sinkt der mögliche Durchsatz sofort auf 50% des Maximalwertes, da eine Antenne nicht gleichzeitig senden und empfangen kann und die Durchsatz-Leistung somit auf einen „Half-Duplex Modus“ reduziert wird, da die Antenne zwischen Sender- und Empfänger-Rolle wechselt. Insofern sind mindestens zwei oder mehr Antennen zu fordern, was jedoch wiederum die Hardware-Kosten erhöht.

Dynamisches Routing:

Dynamische Routing Verfahren wie OSPF setzen eine sehr stabile physikalische Infrastruktur voraus. Die physikalische Infrastruktur (PHY) bei Funkverbindungen ist aber leider von ihrem Wesen her instabil, da ständig Signalschwankungen auftreten. Diese Schwankungen sind dynamisch, asymmetrisch und ändern sich im zeitlichen Ablauf, insbesondere bei beweglichen Knoten (Clients als vermaschte Knoten), aber ebenfalls bei einer fest positionierten Infrastruktur.

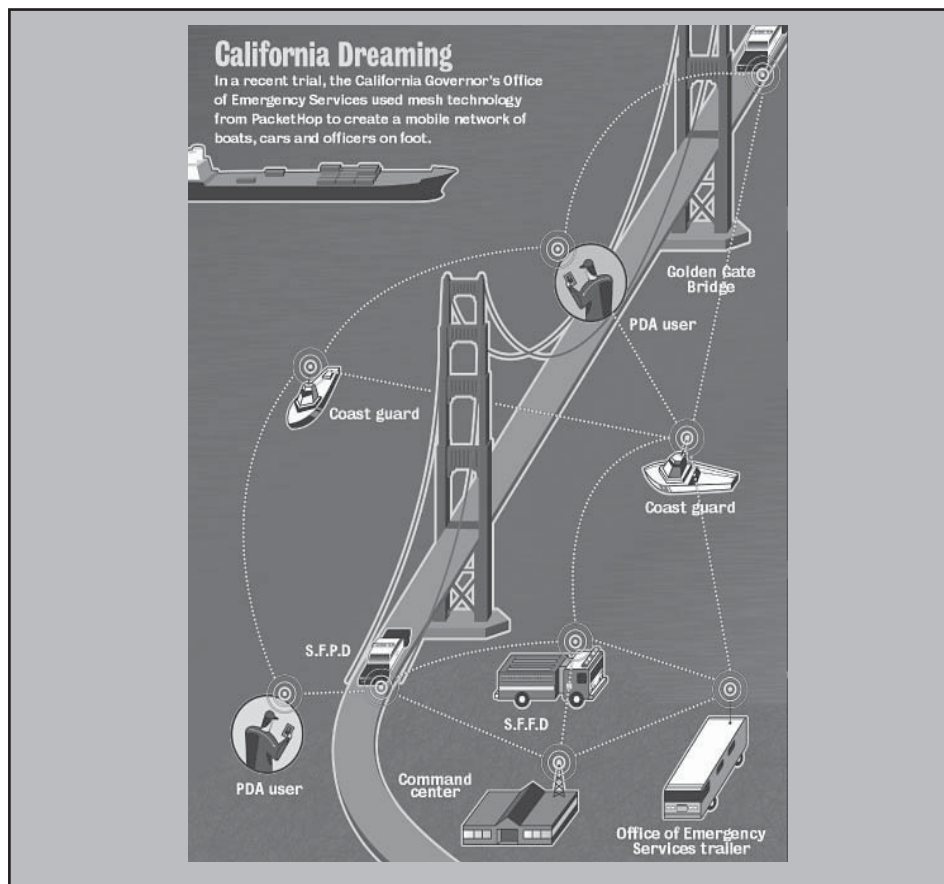


Abbildung 5.11: San Francisco WLAN Pilot für Notfall-Szenarien

Autodiscovery:

Autodiscovery bzw. die Netzlast, die durch Autodiscovery generiert wird, wenn jeder Mesh Knoten „Hallo - ich bin hier“ ruft, ist eines der klassischen Probleme in vermaschten WLAN Netzen, das sich nur durch sehr effiziente Algorithmen handhaben lässt.

Client Systeme als Mesh Knoten:

Werden Client Systeme selbst als Knoten des vermaschten WLANs genutzt, so stellen sie vielfach eine Leistungs-Limitierung des gesamten Mesh WLANs dar: Client-NIC's und Treiber sind im Durchsatz limitiert, das Clientsystem muss sowohl den Overhead-Verkehr als auch die Nutzdaten handhaben. Client-Systeme sind jedoch im Gegensatz zu den Anforderungen an Mesh WLAN Knoten vielfach nicht speziell für die Verarbeitung umfänglicher Autodiscovery Informationen, Routing Informationen oder für die Weiterleitung von Fremdpaketen (Relay-Funktion) ausgelegt. Reichweite und Sendeleistung sind bei Client-Systemen oft niedriger als bei Access Points. Insbesondere Stromversorgung und Batterie-Lebensdauer der Clientsysteme sind ein limitierender Faktor der Gesamtleistung. Somit ist bei Client-Knoten in einem vermaschten WLAN häufiger mit

dem Wegfall einzelner Knoten aufgrund von Mobilität oder Ende der Batterie-Lebensdauer zu rechnen.

Preise:

Die Hardware-Preise liegen im Vergleich zu herkömmlichen WLAN AP's mit z.B. 1.600,- EUR für „Client-Knoten“, 700,- EUR bis 1.500,- EUR für Indoor-AP's und 1.500,- EUR, 2.600,- EUR, 3.300,- EUR, 3800,- EUR bis 7.500,- EUR für Outdoor AP's (BelAir, Cisco, D-Link, FireTide, Tropo) je Backbone-AP relativ hoch und sind vergleichbar mit einem kompletten nicht-modularen Gbit Ethernet Switch (Anm. d. Verf.: Der EUR/USD Kurs wurde mit 1,20 USD/EUR gerechnet).

5.5 Multivendor Mesh WLANs, Interoperabilität?

Aktuell ist der Informations-Austausch der Backbone AP's hinsichtlich Format und Inhalt ausgesprochen proprietär, Gleiches gilt für die „Best Path“ Routing Verfahren (z.B. ATP/MSR, AWPP, PWRP, WITnet, WMN). Die Vorstellung, vermaschte WLANs mit einem Hersteller Mix and Match zu fahren, ist daher noch Zukunftsvision. Diese Vision will der zukünftige Standard IEEE 802.11s zum Leben erwe-

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

cken, der Vorschläge für eine Erweiterung des MAC-Layers mit folgender Maßgabe eingeholt hat: Spezifikation von Unicast und Multicast/Broadcast Weiterleitung unter Nutzung von Metriken auf der Basis aktueller Funkparameter und unter Nutzung selbstkonfigurierender Multi-Hop Topologien mit gleichzeitiger Erweiterung von IEEE 802.11i (Sicherheit) auf die vermaschte Topologie. Erfolgreiche Start Up Firmen wie BelAir, FireTide oder Tropos waren bei der Einreichung von Vorschlägen sehr zurückhaltend mit der Offenlegung ihrer Betriebsgeheimnisse, was Autodiscovery, Auto-konfiguration und Best-Path Algorithmen betrifft - was ja auch letztlich verständlich ist. Möglicherweise wird der Standard Schnittstellen und Formate definieren, die den eigentlichen Algorithmus offen bzw. implementierungs-spezifisch lassen.

6. Erweiterte Anforderungen: Trennung von Benutzergruppen, QoS

6.1 VLAN- und IP Subnetz-Konzepte

Sowohl gesteigerte Netzwerkanforderungen hinsichtlich Verfügbarkeit, Sicherheit und Quality of Service einerseits als auch die Integration von Wireless Technologien andererseits führt vielfach zu Designvorschlägen (besonders von Herstellerseite) mit einer Aufteilung in viele Benutzergruppen, die physikalisch oder mittels VLAN Technik in verschiedene IP Subnetze separiert werden. Insbesondere die Konzeptvorschläge von Herstellern forcieren vielfach

- separate Voice / IP Telefonie VLANs
 - für Sicherheit
 - für QoS
 - für Verfügbarkeit
- separate WLAN VLANs
 - für Sicherheit
 - für QoS im Zusammenhang mit IP Telefonie
- separate Management VLANs
 - für Sicherheit

Zum Thema „Trennung von Benutzergruppen“ gibt es mehrere Insider Beiträge, z.B. Markus Schaub: „Trennung von Benutzergruppen - Lösungen und ihre Folgen“ (Insider Januar 2006) und Petra Borowka: „Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, MAN, RAN; Teil 3“ (Insider Juni 2005), auf die an dieser Stelle für weitergehende Details verwiesen wird.

Das wesentliche Ergebnis sei an dieser Stelle zusammengefasst: Wichtigstes Prinzip für den erfolgreichen Betrieb von Benutzergruppen-Trennung mittels separater VLAN's / IP Subnetze ist das KISS Prinzip: Einfache Regeln, Übersichtlichkeit,

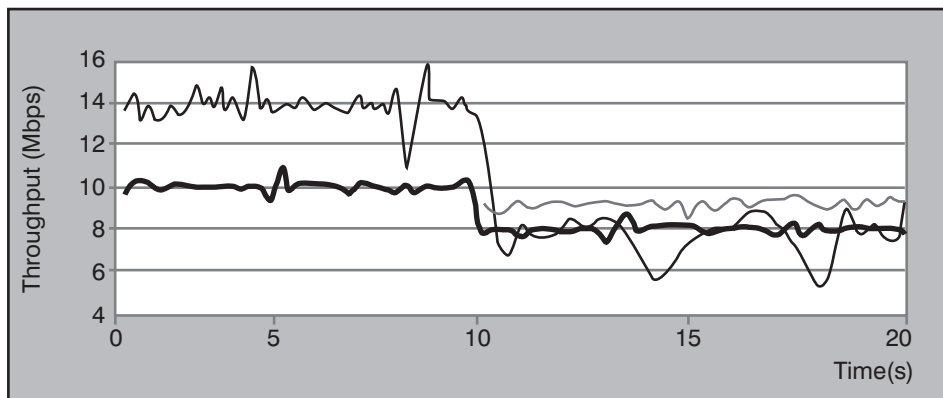


Abbildung 6.1: Datenanwendung führt zur Beeinträchtigung von Video

möglichst technologisch-generische Trennungen wie die Trennung zwischen Wireline (Ethernet) und Wireless (WLAN), Minimierung der Anzahl notwendiger VLAN's, Vermeidung einer Trennung nach Gerätetypen („Telefon“, PC's) und Vermeidung benutzerspezifischer Einzelregelungen.

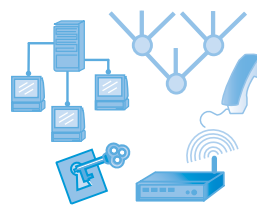
6.2 Quality of Service: IEEE 802.11e und WMM

Für Wireline LAN (Ethernet) Umgebungen wurde in vorausgegangenen Beiträgen mehrfach dargelegt, dass Quality of Service in Ethernet / IP LAN Switches sehr wohl verfügbar ist, jedoch in den meisten Fällen gewichteter 100Mbit/1Gbit-Netze aktuell kein ernsthaft nachweisbarer Bedarf für eine QoS-Implementierung mittels Pri-

orisierung, Bandbreitenreservierung und Policy-Definitionen vorliegt (dies gilt nicht für WAN-Verbindungen!).

Bei Wireless LANs stellt sich die Situation jedoch anders dar: Da es sich hier um eine Shared LAN Technologie mit immant schwankender Signalstärke und somit Datenrate handelt, die zudem aktuell mangels verfügbarem Gbit WLAN keine hohen Überkapazitäten bereitstellt, ist von Dienstgüte-Schwankungen auszugehen, die beim Betrieb kritischer Anwendungen ohne weitergehende QoS-Maßnahmen erkennbar zu Qualitäts-Einbußen führen. Wachsende Verbreitung von WLANs und die Verfügbarkeit von WLAN Telefonen sowie anderen WLAN-fähigen Multimedia-Ge-

Netzwerk-Redesign-Forum 2006



**27.03. - 30.03.06
in Königswinter**

Das Netzwerk-Redesign Forum, unser Top-Kongress des Jahres 2006, analysiert die aktuellsten Entwicklungen der Netzwerk-Technologien und bewertet Markttrends und Produktentwicklungen. Wir blicken für Sie hinter die Kulissen, geben Erfahrungsberichte aus aktuellen Projekten und bewerten die Praxis-Relevanz der neuesten Trends.

Mit den wachsenden Anforderungen an Netzwerke hat sich das Design moderner Netzwerke immer weiter gewandelt. Im Wesentlichen basiert dieser Wandel auf 5 Kernfaktoren:

- Erhöhte Leistung in Kombination mit erhöhter Verfügbarkeit
- Vorbereitung auf IP-Telefonie (Voice-ready) und weitere neue IP-basierte Dienste
- Architektonische Integration von WLANs
- Sicherheit in mehreren Stufen auf Netzwerk-Ebene
- Vorbereitung auf Service-Management für ausgewählte Services

Moderation: Dr. Jürgen Suppan

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

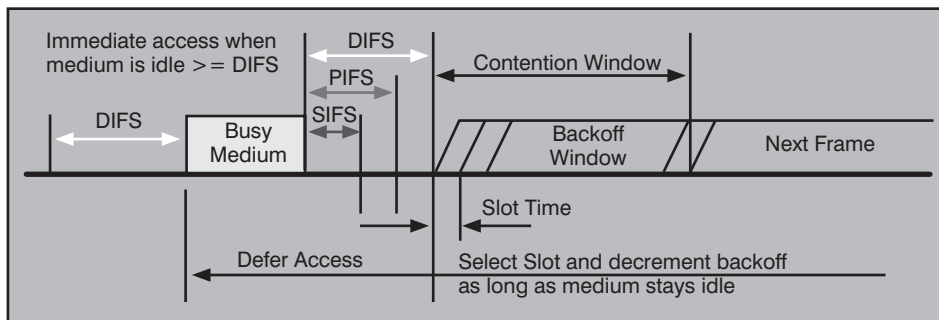


Abbildung 6.2: Abhängigkeit des Kanalzugriffs vom Inter-Frame Spacing

räten (Video-Überwachung etc.) führten zu einem Bedarf nach QoS-Funktionalität in WLAN-Infrastrukturen. Das Beispiel aus Abbildung 6.1 zeigt im zeitlichen Ablauf zuerst zwei Sessions, eine Datensession und eine Videosession. Die Summenleistung beträgt ca. 26 Mbit/s, beide Applikationen haben noch den erforderlichen Durchsatz. Nach etwa 10 Sekunden startet eine dritte Session und entzieht, da gleichberechtigt, den beiden vorhandenen Sessions so viel Leistung, dass die Videosession eine Qualitäts-Einbuße erleidet.

Der IEEE 802.11 Basis-Standard kennt zwei Verfahren: das verteilte zufallsgesteuerte DCF (Distributed Coordination Function) für Best Effort und das zentral gesteuerte PCF (Point Coordination Function), bei dem die beteiligten Clients intervallmäßig von einem Master gepollt werden (SNA lässt grüßen...) und bei Sendebedarf ein Senderecht für ein bestimmtes Zeitintervall erhalten. Es sind nun unterschiedliche Interframe Spacings (IFS) spezifiziert, wie Abbildung 6.2 zeigt: PIFS (für PCF, niedrigster Wert), Acknowledgements (SIFS) und DIFS (für DCF). Die unterschiedlich langen Interframe Spacings sorgen zwar für eine gewisse Priorisierung, die jedoch bei weitem nicht ausreicht, da z.B. bei allen Datenübertragungen, die ja das DIFS nutzen müssen, keine weitere Unterscheidung möglich ist. PCF hat sich jedoch nicht durchgesetzt und ist als historisch zu bewerten.

IEEE 802.11e spezifiziert mehrere Erweiterungen der bisherigen DCF. Nachfolgend wird zuerst EDCF als Priorisierungs-Verfahren näher erläutert, da die Wi-Fi Allianz für diese Funktion vorab ein Profil und Interoperabilitätstests erarbeitet hat und es inzwischen verfügbare Produkte mit dieser Funktion gibt (z.B. von Cisco, Enterasys, SpectraLink).

IEEE 802.11e / WMM Überblick

Im Vorfeld der Verabschiedung des QoS-Standards IEEE 802.11e definierte die Wi-Fi Allianz WMM (Wi-Fi Multimedia) als IEEE 802.11e Profil zur Abdeckung der dringendsten QoS-Bedarfe, nämlich dem Be-

trieb von VoFi (IP Telefonie über IEEE 802.11 WLAN). WMM- / IEEE 802.11e-Funktionalität muss stets auf beiden Seiten einer WLAN-Verbindung, d.h. sowohl im Client Adapter als auch im Access Point unterstützt werden. Zur Verbesserung und Sicherstellung der Interoperabilität verschiedener Produkte hat Wi-Fi ein Programm zur WMM Zertifizierung entwickelt, die vom Anwender gefordert werden sollte, falls er QoS nutzen will.

IEEE 802.11e / WMM erweitert Wi-Fi Netze um QoS-Funktionalität im Sinne optimierter Leistung bei parallelem Betrieb unterschiedlich kritischer Anwendungen, was WMM dadurch erreicht, dass auf der Basis von Enhanced Distributed Channel Access (EDCA) eine unterschiedliche Priorisierung für den Medien-Zugang zur Verfügung gestellt wird. Vorteile von WMM sind:

- Interoperabilität zwischen verschiedenen
 - Gerätetypen
 - Herstellern
- Verfügbarkeit der Spezifikation und Testpläne seit Ende 2004
- Zusammenarbeit mit IEEE 802.11e; Spezifikation von WMM als Untermenge des IEEE 802.11e Drafts
- Breite Einsetzbarkeit: nicht nur im En-

terprise Umfeld sondern auch im SOHO und öffentlichen Carrier Markt, was die Verbreitung von WMM zertifizierten Produkten zusätzlich fördert

- Koexistenz mit non-WMM Komponenten im selben WLAN Netz
- Gute Anpassung an dynamische Datenraten
- Nutzung der IETF DiffServ Architektur, Nutzung von IETF DSCP Headern und IEEE 802.1D Tags
- Kompatibilität mit Universal Plug and Play (UPnP) QoS

Priorisierung und Queues bei WMM / IEEE 802.11e

IEEE 802.11e / WMM definiert zur Verkehrssteuerung vier Prioritätsklassen als Zugangsklassen (AC, Access Categories): Voice, Video, Best Effort und Background, wobei Voice die höchste, Background die niedrigste Priorität darstellt (hoher Wert = hohe Priorität, niedriger Wert = niedrige Priorität). Die AC's sind aus dem IEEE Standard 802.1D abgeleitet, daher hat Sprache höhere Priorität als Video. Der Zusammenhang zwischen IEEE 802.1D und WMM AC's ist in Abbildung 6.3 dargestellt. Die dargestellte Zuordnung von Applikationen zu AC's sind der WMM Vorschlag und sind auf spezifische Verkehrstypen zugeschnitten (Sprache, Video, Best Effort und niederpriorige Daten). Sie soll insbesondere auch die Kompatibilität zu aktuell eingesetzten Policy Tools ermöglichen (z.B. UPnP). Im konkreten Einsatzfall kann der Betreiber durch entsprechende Policies die AC-Werte 1 bis 4 auch anderen Anwendungen zuordnen, bei einigen Herstellerlösungen ist jedoch Netzwerkmanagement fest auf den höchsten Wert „4“ (IEEE „7“) konfiguriert.

Die QoS-Funktionalität in IEEE 802.11e / WMM ist als Verbesserung des MAC Sublayer implementiert und ist eine Erweite-

IEEE 802.11e / WMM Zugangs-Kategorien		
Access Category	Beschreibung	IEEE 802.1D Werte
WMM Voice Priority	Höchste Priorität, ermöglicht mehrere bis viele parallele Gespräche (Calls) mit TDM-Qualität	7,6
WMM Video Priority	Priorisierung von Video-Sessions gegenüber Daten-Sessions; Ein 802.11g oder 802.11a Kanal kann 3-4 SDTV Datenströme oder 1 HDTV Datenstrom unterstützen (!)	5,4
WMM Best Effort Priority	„Normale“ = unkritische Anwendungen oder Anwendungen, die QoS nicht unterstützen; Anwendungen, die weniger Delay-sensitiv sind, jedoch keine übermäßig hohen Antwortzeiten haben sollen (Bsp. Web-Surfen)	0,3
WMM Background Priority	Niederpriorige Anwendungen wie Downloads, Druckjobs, die keine strikten Antwortzeit- und Durchsatz-Anforderungen haben	2,1

Abbildung 6.3: WMM Zugangs-Kategorien

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

zung des normalen CSMA/CA-basierten DCF Verfahrens, das nach dem „Erst horehen, dann reden“ Best-Effort-Algorithmus arbeitet und allen Geräten / Benutzern dieselbe Priorität gibt: Jeder Client wartet eine zufällige Backoff-Zeit und fängt danach nur dann an zu senden, falls kein anderes Gerät sendet. Bei höheren Lasten erleidet dieses Verfahren noch höhere Leistungseinbußen als der CSMA/CD Algorithmus von Shared Ethernet. Mit IEEE 802.11e / WMM wird jedes Paket / Frame einer AC zugeordnet, je AC wird geräteintern eine separate Queue vorgehalten. Pakete innerhalb einer Queue sind gleichberechtigt, Pakete in Queues mit höherem AC-Wert sind gegenüber Queues mit niedrigerem AC-Wert bevorzugt. Der MAC Client implementiert eine interne Kollisions-Handhabung (Collision Resolution), die dafür sorgt, dass als nächstes Paket eines mit der aktuell höchsten Priorität gesendet wird. Dasselbe Verfahren handhabt externe Kollisionen, um zu entscheiden, welcher Client als nächstes die Gelegenheit zum Senden erhalten soll (TXOP, Transmission Opportunity).

Warte- und Sendezeiten

Die Kollisions-Resolution, die die Verkehrspriorisierung regelt, arbeitet wahrscheinlichkeits-gesteuert und das Ergebnis hängt von zwei Timern ab, die für jede Access Category unterschiedlich gesetzt sind:

- das minimale Interframe Spacing bzw. Arbitrary Inter-Frame Space Number (AIFS)
- das Kollisionsfenster CW (Contention Window), manchmal als Random Back-off Wait bezeichnet

Beide Timer sind umso kleiner, je höher der AC-Wert ist, d.h. je höher die Priorität des Frames ist. Für jede Zugangs-Kategorie wird der Backoff Wert als Summe aus AIFS und einem Zufallswert zwischen 0 und CW berechnet. Es gilt: AIFS ist immer größer als der DIFS-Wert aus DCF, CW[AC] für Voice und Video ist kleiner als der CWMIN-Wert aus DCF.

Die Wartezeit W beträgt also

$$W = AIFS[AC] + CW_{\min}[AC] \dots AIFS[AC] + CW_{\max}[AC] \text{ mit } AIFS[j] < AIFS[i] \text{ für } i < j$$

mindestens

$$W = AIFS[AC]$$

maximal

$$W = AIFS[AC] + CW_{\max}$$

Der CW-Wert wird auf einen Anfangswert gesetzt, der von der AC abhängig ist und ändert sich mit fortschreitender Wartezeit: Nach jeder Kollision wird der CW-Wert verdoppelt bis zur Erreichung eines Maximalwerts, der ebenfalls AC-abhängig ist. Nach einem erfolgreichen Sendevorgang, wird der CW-Wert auf den Anfangswert zurückgesetzt. Jeweils die Zugangs-kategorie mit

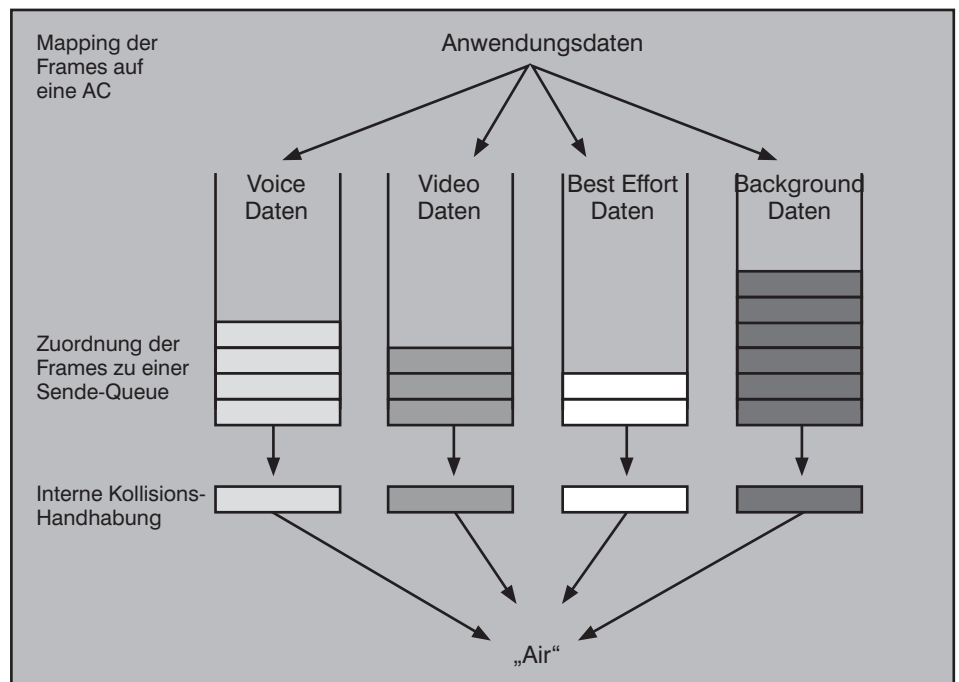


Abbildung 6.4: Queues der vier AC's in einem IEEE 802.11e / WMM Client

Achtung: Wie in Abbildung 6.4 deutlich wird, können höherpriorige Warteschlangen die niederpriorigen Warteschlangen erheblich benachteiligen, wenn sie einen hohen Gesamtlast-Anteil haben! Daher sollten die AC-Werte mit der gebotenen Vorsicht gesetzt und hohe AC-Werte nur bandbreiten-genügsamen Anwendungen zugeordnet werden.

dem niedrigsten berechneten Backoff Wert erhält die Sendegelegenheit (TXOP).

Die Wartezeit wird in Einheiten von Slotzeiten (Slot-Time) berechnet, die Slot-Time für IEEE 802.11a/g beträgt 9 Mikrosekunden, die Slot-Time für IEEE 802.11b beträgt 20 Mikrosekunden. Eine Übersicht zeigt Abbildung 6.5.

wenn sie mit Geräten um den Medienzugang konkurrieren, die nur eine niedrigere PHY Datenrate unterstützen (z.B. aufgrund größerer Entfernung). Mit WMM ändert sich das Beispiel aus Abbildung 6.1 zu Abbildung 6.6: Die Videosession läuft über das gesamte Zeitintervall hinweg mit gleich bleibender Qualität, die Datensessions erhalten niedrigeren Durchsatz und „teilen“ sich die verbleibende Bandbreite.

Beispiele:

Ein WLAN Telefon mit 802.11b Schnittstelle hat eine Wartezeit von	2 – 5 Slots	40 – 100 µs
Ein WLAN Telefon mit 802.11a/g Schnittstelle hat eine Wartezeit von	2 – 5 Slots	18 – 45 µs
Eine nichtpriorisierte Anwendung über 802.11b Schnittstelle wartet	3 – 18 Slots	60 – 360 µs
Eine nichtpriorisierte Anwendung über 802.11a/g Schnittstelle wartet	3 – 18 Slots	27 – 162 µs
Ein Batchjob (Background) 802.11b Schnittstelle wartet	7 – 22 Slots	140 – 440 µs

Weitere IEEE 802.11e Funktionen

Im Vergleich zu Basis-WMM enthält IEEE 802.11e weitere QoS Funktionen:

- Zentral gesteuertes Polling mit HCF/HCCA
- Direct Link Setup (DLS) / Direct Link Protocol (DLP) für die direkte Kommunikation zwischen zwei Stationen unter Umgehung des Access Points
- Block Acknowledgement
- No Acknowledgement
- Power Save

Mit Erhalt einer TXOP hat ein Client die Erlaubnis, eine bestimmte Zeit lang zu senden. Diese Sendezeit ist wiederum abhängig vom AC-Wert und der PHY Datenrate. Diese Burst-Regelung erhöht die Effizienz für Verkehrslasten mit hohen Datenraten erheblich (z.B. AV Streaming). Außerdem werden Geräte, die mit einer höheren PHY Datenrate laufen, nicht benachteiligt,

Netzwerk Design 2006: Anforderungen, neue Technologien, Trends

Beispiele: das TXOP Intervall liegt in den Bereichen

0,2 ms (Background) .. 3 ms (Video) in einem 802.11 a/g Netzwerk
1,2 ms (Background) .. 6 ms (Video) in einem 802.11 b Netzwerk

bis ausreichend deterministische Überkapazität wie beim geschalteten LAN verfügbar ist. Dies gilt insbesondere für den Einsatz von Telefonie / Sprache (VoFi).

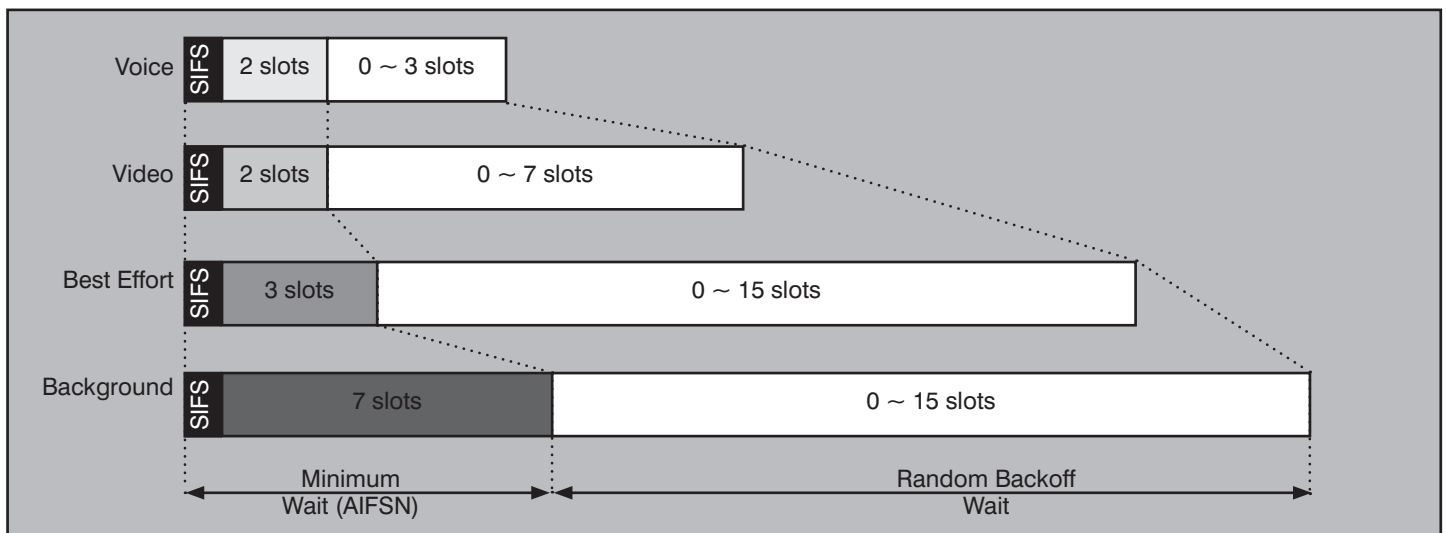


Abbildung 6.5: WMM AC Timerwerte

HCF erlaubt es Anwendungen, abhängig von ihren Verkehrs-Charakteristiken Netzwerkressourcen zu reservieren. Sie tun dies mit dem Polling Verfahren HCCA (HCF Controlled Channel Access), bei dem der Client entsprechende Requests an den Access Point (AP) sendet und der AP dem Client TXOP's zurück gibt, die zur jeweiligen Anwendung passen. Die TXOP-Zuweisung ist abhängig von mehreren Parametern der Sendespezifikation (TSPEC, Transmission Specification) wie Datenrate, PHY Rate, Framengröße, Service-Intervall, Burstgröße. Das Polling unterstützt so einen parametrisierten planmäßigen Mediezugang. Da hier niedrigere Backoff Delays auftreten, kann HCCA mit der Nutzung eines zentralen Scheduling Kontrollverfahrens die durchschnittliche Antwortzeit reduzieren. Allerdings erfordert der Einsatz von HCF im Unterschied zu Basis-WMM, dass das

Clientsystem vorher weiß, welche und wie viele Ressourcen es benötigt, und dass der Access Point gewisse Annahmen trifft, um konkurrierende Verkehrslasten effizient zu handhaben. Solche Annahmen sind z.B. minimale vs. maximale Framengröße, minimale vs. maximale PHY Rate, Startzeit oder zusätzliche Bandbreiten-Reservierung bei Sende-Wiederholungen.

Fazit

WLAN-Komponenten erhalten zunehmend QoS-Funktionalität, der Markttrend geht hier in Richtung IEEE 802.11e / WMM, proprietäre Verfahren wie SVP werden mittelfristig verschwinden. QoS für WLANs ist bei Einsatz kritischer und zeitkritischer Anwendungen derzeit unverzichtbar, da Anwender auf diese Anwendungen nicht so lange warten wollen,

Links

www.cisco.com
www.nortel.com
www.tropos.com
www.motorola.com
www.meshnetworks.com
www.packethop.com/products/truemesh_software.php
www.accton.com/homepage
www.belairnetworks.com
www.d-link.de
www.firetide.com
www.interdigital.com
www.nexthop.com
www.packethop.com
www.strixsystems.com
www.thomson.com
grouper.ieee.org/groups/802/11/
grouper.ieee.org/groups/802/16/
www.wimaxforum.org
www.wi-mesh.org

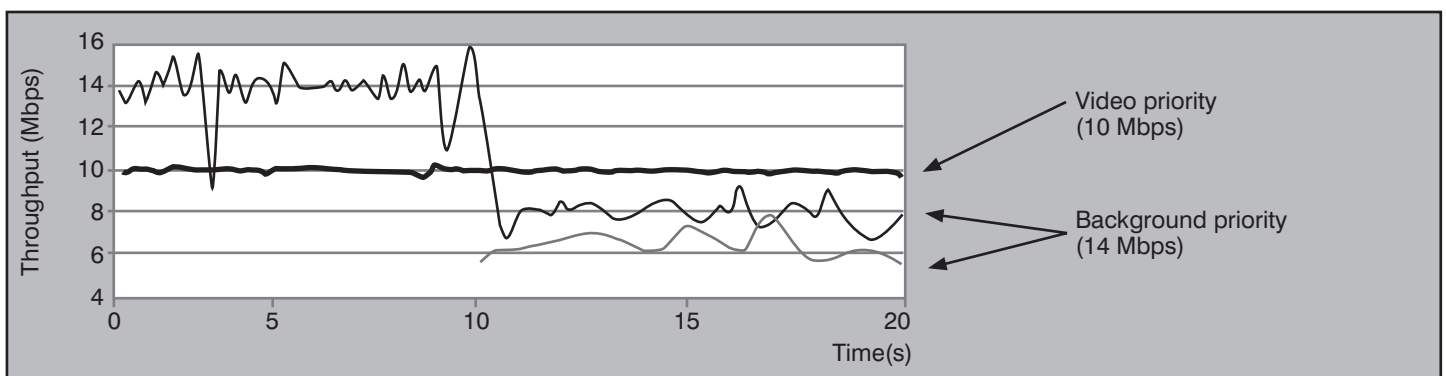


Abbildung 6.6: Einsatz von IEEE 802.11e / WMM führt zur Priorisierung von Video gegenüber den Datensessions

CCNE

ComConsult Certified Network Engineer

Lokale Netze

03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

Internetworking

08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP

15.05. - 19.05.06 in Stuttgart
25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand

29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 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

08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen

27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen

24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 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

15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb

19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clients, WLANs

03.04. - 07.04.06 in Aachen
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

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



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

Impressum

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

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

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungsweise: 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
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research