Dr. Suppan International Institute

Der Netzwerk Insider

April 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

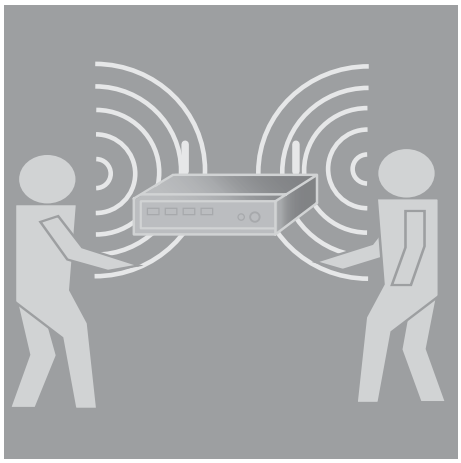
Schwerpunktthema

Angriff auf DECT Voice over WLAN

von Dr. Simon Hoff

Je mehr WLAN nach IEEE 802.11 flächendeckend im betrieblichen oder im privaten Bereich im Einsatz sind, desto interessanter und berechtigter ist die Frage der Sprachübertragung über WLAN.

Der Hintergrund ist klar: Natürlich möchte man, wie man es ja von der Festnetzseite gewohnt ist, am liebsten über eine einzige Infrastruktur alle Dienste abwickeln können und nicht für drahtlose Sprach- und Datendienste unterschiedliche Netze aufbauen müssen. Einfach ist diese Integration im Bereich der Funknetze allerdings nicht, denn physikalische Übertragung und Kanalzugriff müssen hier empfindlich



auf die charakteristischen Eigenschaften des zu erbringenden Diensts abgestimmt sein. In diesem Artikel wird zunächst der aktuelle Stand der Standardisierung zur Erweiterung von WLAN nach IEEE 802.11 um Quality-of-Service-Konzepte erörtert. Anschließend werden anhand eines konkreten Produktbeispiels die Möglichkeiten und Tücken der Sprachübertragung im WLAN im Detail analysiert. Dabei wird sich zeigen, dass Voice over IP over WLAN den Nischenmarkt verlassen hat und auch entsprechend professionelle Produkte am Markt verfügbar sind.

weiter auf Seite 17

Zweitthema

Übertragung von SIP über Firewalls

von Dr. Behrooz Moayeri

Nicht nur die große Mehrheit der Hersteller im Bereich Voice over IP (VoIP), sondern auch Provider und Microsoft setzen auf das Session Initiation Protocol (SIP) als den Standard für die Kommunikation von Person zu Person.

Das 3rd Generation Partnership Project (3GPP), der Zusammenschluss von Anbietern im Bereich des Mobilfunks dritter Generation, hat sich bereits vor Jahren auf SIP als Signalisierungsstandard im IP-Bereich festgelegt. Real Time Communication (RTC) von Microsoft basiert auf SIP und ist in den Messenger von Windows XP integriert.

SIP-Anwendungen beschränken sich nicht nur auf Telefonie und Fax, sondern umfassen mittlerweile Präsenz-basierende Applikationen, Videokonferenzen und Dateiaustausch von Peer to Peer. Auch Spiele lassen sich mit SIP starten.

Bei der Implementierung von SIP gibt es jedoch einige Probleme zu lösen, allen voran die komplexe Aufgabe der Behandlung einer Kommunikation von außen nach innen durch eine Firewall. Viele Peer-to-Peer-Anwendungen wie VoIP arbeiten mit dynamischen UDP-Ports. Eine Firewall, die den ganzen infrage kommenden Portbereich ständig offen halten würde, verdiente den Namen Firewall nicht.

weiter auf Seite 6

Top-Event

Das ComConsult IT-Sicherheits-Forum 2004

auf Seite 4

Zum Geleit

Embedded Devices und RFID erfordern erweiterte Netzwerk-Infrastrukturen

auf Seite 2

Report des Monats

IT-Infrastrukturen: Ergebnisse einer Umfrage

auf Seite 15

Zum Geleit

Embedded Devices und RFID erfordern erweiterte Netzwerk-Infrastrukturen

Unbemerkt von der breiten Öffentlichkeit entwickelt sich ein Technologie-Bereich in einer enormen Geschwindigkeit weiter, der einerseits bestehende Logistik-Abläufe optimiert und andererseits erhebliche Anforderungen an Integrations-Infrastrukturen stellen kann.

Im Rahmen dieses Geleitworts soll dieser Technologie-Bereich differenziert werden in die Teilbereiche:

- Embedded Devices: Integration kleiner, preiswerter Computer-Steuerungen, typischerweise auf der Basis eines Linux-Derivats in Maschinen beliebiger Art.
- RFID: Radio Frequency Indentification, auch SmartTag-Technology genannt. Unter diesem Begriff werden Markierungen von Waren, Personen oder sonstigen Gegenständen verstanden, die über Funk abgefragt werden können. Typisch sind Aufkleber in Warenhäusern.

Bei den Embedded Devices ist davon auszugehen, dass speziell in Anwendungsbereichen, in denen Service-Vorgänge optimiert werden können (Automatisierung von Service-Vorgängen und Störungs-Bearbeitung an Maschinen, Remote Service Fähigkeit), eine relativ schnelle Verbreitung erfolgt. Die stark sinkenden Preise einerseits und die zunehmende Verbreitung von Linux andererseits senken die Einstiegsschwelle in diese Technologie rapide. Die bei Embedded Devices durch die Wahl des Betriebssystems gegebene Einbindungsfähigkeit in Datennetze führt fast zwangsläufig zur Frage nach entsprechenden Integrations-Infrastrukturen.

Wesentlich kritischer ist aber ohne Frage die Entwicklung im Bereich RFID. Diese Technik ist nicht neu, sie wird zum Diebstahlschutz in Kaufhäusern oder zur Kennzeichnung von Containern schon längere Zeit eingesetzt. Bisher haben aber die relativ hohen Kosten pro Tag und der nur beschränkte Speicherraum in Kombination mit fehlenden Standards zur Nummerierung und Informationsspeicherung (Weiterentwicklung und Verfeinerung von Barcodes) eine massive Verbreitung verhindert. Doch eine erwartete Einsatzmenge von 1 Milliarde Tags in 2004, nachdem für dieselbe Zahl von Tags zuvor über 15 Jahre benötigt wurden, zeigt, dass hier in

vielen Bereichen eine ausreichende Wirtschaftlichkeit erreicht wird und eine Welle auf uns zukommt. Für das Jahr 2015 sprechen Prognosen von Installationsmengen im Billionen-Bereich.

Die Einsatzbereiche der RFID-Tags sind von folgenden Faktoren abhängig:

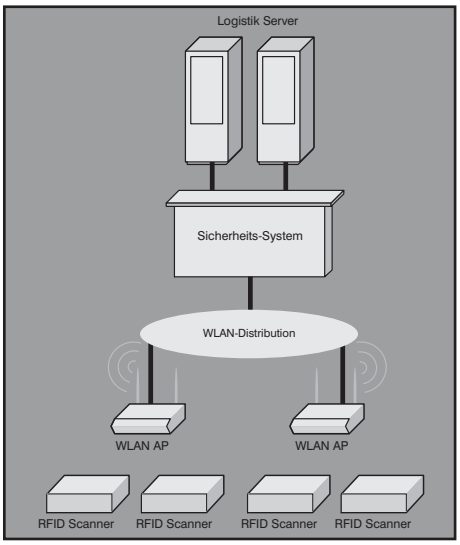
- Preis pro Tag
- Reichweite der Abfragefähigkeit
- Informationsumfang und Typ der Information (im Labor wird an der Integration von Sprachinformation gearbeitet)
- Art der Befestigung

Mit sinkenden Preisen wird die RFID-Flut kommen. Das amerikanische Militär schreibt inzwischen de Kennzeichnung von Waren mit RFID-Tags vor, in Deutschland wird eine generelle Einführung bei der Metro seit Wochen kontrovers diskutiert. Die Konsequenzen für den Bereich Warenlogistik wären: eine komplette Palette kann am Wareneingang gescannt werden (bis zu 1000 Tags sind gleichzeitig lesbar), die gesamte Lagerhaltung, aber auch Warenpräsentation im Verkaufsbereich kann wesentlich erweitert werden und in der Warenwirtschaft kann jeder einzelne Gegenstand mit allen bisherigen Bewegungen und dem aktuellen Standort abgerufen werden. Auch der Kassenbereich dürfte sich mit dieser Technologie verändern. Man stelle sich einen Kunden mit einer RFID-Kundenkarte in der Tasche vor, der einfach seinen Einkaufswagen durch eine Zahlschleuse schiebt und damit automatisch bezahlt. Spätestens an diesem Beispiel wird der Einfluss dieser Technologie auf die Arbeitsplatzsituation deutlich. Mit einer erweiterten RFID-Nutzung werden erhebliche Mengen an Arbeitsplätzen wegfallen.

In Deutschland wird diese Technologie vor allem von den Datenschützern diskutiert. Die Kombination aus RFID-Kundenkarte und Waren, die einzeln einem Kunden zugeordnet werden können, führt zweifelsfrei zu einem gläsernen Kunden. Doch diese Erkenntnis ist nicht so neu. Wer heute mit einer Kundenkarte bezahlt, wie in der Metro üblich, dem können heute schon die gekauften Warengruppen zugeordnet werden, nur nicht individuelle Waren.

Das Jahr 2004 wird in Deutschland das Jahr der Vorbereitung auf RFID sein. Signifikante Vorreiter wie die Metro (inklusive der zum Konzern gehörenden Warenhäuser) werden eine entsprechende Nutzungswelle auslösen. In den USA ist diese Phase bereits vorbei und eine flächige Verbreitung ist nicht mehr in Frage zu stellen. Wenn Zulieferer einmal damit begonnen haben, Waren durchgängig mit RFID zu kennzeichnen, ist die Nutzung der damit verbundenen Möglichkeiten nur noch eine Frage der Zeit.

Damit entsteht für viele Unternehmen die Frage nach der erforderlichen Infrastruktur zur technischen Integration der RFID-Information in die Warenwirtschafts-IT. Dies betrifft nicht nur Warenhäuser, auch



Embedded Devices und RFID erfordern erweiterte Netzwerk-Infrastrukturen

im Gesundheitsbereich sieht man enorme Einsatzpotenziale für diese Technologie. RFID-Lesegeräte müssen in eine IT-Gesamtlösung eingebunden sein, nur dann machen sie Sinn. Da der Standort der Lesegeräte speziell im Warenhausbereich massiven Schwankungen unterworfen ist, kann eine Integration sinnvoll nur durch Wireless Technik erfolgen.

RFID wird in Konsequenz zu einer starken Ausbreitung flächendeckender Wireless-Netzwerke führen. Hier schließt sich jetzt die Argumentationskette, da dies auch für den Bereich der Embedded Devices gilt. Vereinfacht ausgedrückt ist WLAN-Technologie eine Schlüssel-Technologie für die Optimierung bestehender Arbeits- und Logistikabläufe.
Und dies ist das zentrale Anliegen dieses Geleitworts. WLANs werden heute in vielen Fällen auf einem sehr einfachen Niveau mehr als Punktlösung installiert. Die Sichtweise einer flächendeckenden strategischen Technologie ist nicht allgemein verbreitet. Sehr wohl sehen die Anbieter von WLAN-Technologie diesen strategischen Anspruch. WLAN-Produkte werden durch die professionellen Anbieter in einer Form angeboten, die diesem strategischen Anspruch genügt. Auch die weiteren bis Mitte des Jahres zu erwartenden Produkte werden speziell in diese Richtung marschieren.

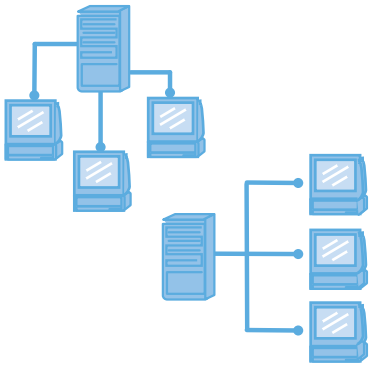
Mit den WLANs als strategische Infrastruktur sind aber auch die Strukturen vieler bestehender Netzwerke überfordert. Ein Redesign der Strukturen und der Konfiguration ist unvermeidlich. Dieser Bedarf entsteht auch aus anderen Entwicklungen, wie zum Beispiel dem Eindringen von Ethernet in den Feldbusbereich oder der jetzt einsetzenden Massennutzung von IP-Telefonie. Die Netzwerk-Strukturen der letzten 10 Jahre sind nicht in jedem Fall geeignet, diese Entwicklungen zu tragen. Eine Revision ist dringend erforderlich.

Wie unterstützen wir Sie bei diesen Entwicklungen:

- Die RFID-Entwicklung wird von uns aus dem Labor von ComConsult-Research begleitet
- Das Seminar über Wireless-LAN zeigt auf, welche Infrastruktur-Anforderungen durch WLANs gestellt werden und wie diese gelöst werden
- Das Seminar Design Lokaler Netzwerke behandelt speziell den Bereich des Redesign bestehender Netzwerke, um diesen Entwicklungen Rechnung zu tragen

Ihr
Dr. Jürgen Suppan

Seminar zum Thema



Design-Varianten Lokaler Netzwerke im Vergleich

Seminar

14.06. - 16.06.04 in Bonn

11.10. - 13.10.04 in Köln

Dieses Seminar vermittelt dem Fortgeschrittenen in 3 Intensiv-Tagen, was ein modernes LAN-Design technisch und wirtschaftlich leistet. 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-Systeme im Sinne von Verfügbarkeit, Loadbalancing und Verkehrs-optimierung architektonisch integriert werden können.
Referentin: Dipl.-Inform. Petra Borowka
Einzelpreis: € 1.690,- zzgl. MwSt.

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

Seminar zum Thema

Wireless LAN: Planung, Produktauswahl, Installation, Trouble Shooting

Seminar

03.05. - 07.05.04 in Zürich-Glattbrugg

14.06. - 18.06.04 in Bonn

12.07. - 16.07.04 in Köln

20.09. - 24.09.04 in Bonn

15.11. - 19.11.04 in Köln

Dieses Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. WLAN-Varianten werden verglichen und Empfehlungen für eine optimale Auswahl gegeben.
Referenten: Dr. Simon Hoff, Dipl.-Ing. Hans Peter Mohn, Dr.-Ing. Joachim Wetzlar
Einzelpreis: € 2.290,- zzgl. MwSt.

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

Thema

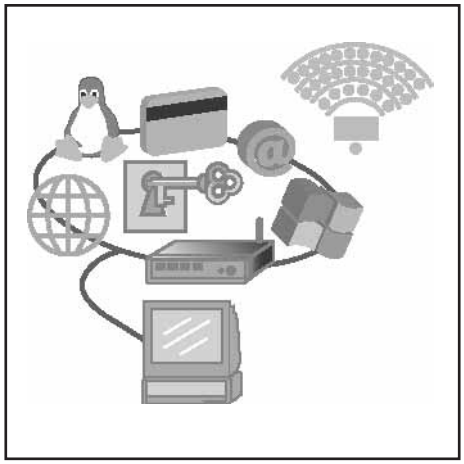
ComConsult IT-Sicherheits-Forum 2004

Vom 10. bis 13. Mai 2004 veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter das „ComConsult IT-Sicherheits-Forum 2004“.

Dieses Forum ist unser herausragendes Event zum Thema IT-Sicherheit im Jahr 2004. Das Programm aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen verbindet die Vermittlung aktuellen Know-hows mit der im Tagesbetrieb benötigten Praxisrelevanz.

Als Schwerpunkte sind in diesem Jahr vorgesehen:

- Webanwendungen mit gravierenden Risiken
- Content-Security: Umgang mit gefährlichen Inhalten
- Erweiterte Sicherung der Netzgrenzen
- Mobility unter Sicherheitsaspekten
- Zentrale Mailverschlüsselung
- Patch- und Updatemanagement
- Sicherheitsstrukturen für interne Netze



IT-Sicherheit in Theorie und Praxis -
Die wichtigsten Entwicklungen
bei Bedrohungen und Schutzmaßnahmen

- Sicherung von WLANs
- Intrusion Detection / Intrusion Prevention
- Auditierung und Zertifizierung
- Praxis-Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei Tutorien (IT-Sicherheit im Überblick, zwei Fachthemen).

Wie in jedem Jahr wird auch 2004 dieser Kongress von Dipl.-Inform. Detlef Weidenhammer, Geschäftsführer der GAI NetConsult GmbH, mitveranstalt und moderiert.

Ausgesuchte Top-Experten der Security-Szene erläutern Ihnen in Erfahrungsberichten aus der unternehmerischen Praxis und in ausgewählten Fachvorträgen die vorhandenen Sicherheitsprobleme und zeigen Ihnen Lösungsmöglichkeiten auf.

ComConsult IT-Sicherheits-Forum 2004

10.05. - 13.05.04 in Königswinter

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

Ich melde an für das
IT-Sicherheits-Forum 2004 in Königswinter

☐ mit Tutorium
vom 10.05. - 13.05.04
zum Preis von 1.990,-- zzgl. MwSt.

☐ ohne Tutorium
vom 11.05. - 13.05.04
zum Preis von 1.690,-- zzgl. MwSt.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

ComConsult IT-Sicherheits-Forum 2004

Montag, 10.05.04 Tutorien

Tutorium 1: IT-Sicherheit im Überblick

- Angriffe in Netzen • Vorbereitung und Angriffstechniken
- Sicherheitsmodell und Sicherheitsgrundfunktionen
- Firewalls, IDS, Virenschutz
- Kryptographische Schutzfunktionen
- Anwendungsbereiche (Authentisierung, Integrität, Verschlüsselung)
- Anwendungsszenarien (VPN, Webserver, E-Mail)
- Aufbau einer Sicherheitsorganisation
- Methodik und Elemente zur Erstellung von Sicherheitskonzepten
- Messbarkeit der Sicherheit, Kriterienkataloge
- Evaluierung und Zertifizierung

Dr. Gerhard Weck, Infodas, Köln

Tutorium 2: Aktuelle Hacking-Techniken - Grundlagen und Praxisbeispiele

- Erstellung des Zielprofils
- Fortgeschrittene Scan-Methoden
- Schwachstellen in Windows-Netzwerken
- Man-in-the-Middle Attacken
- Sniffen in geswitchten Netzen

Andreas Schmidt, Cirosec, Heilbronn

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallel stattfindenden Tutorien.
Alle Tutorien starten um 10:00 Uhr und enden gegen 17:30 Uhr.
Bitte kreuzen Sie Ihr bevorzugtes Tutorium an.

Tutorium 3: Erstellung einer Security Policy

- Zieldefinition für eine Security Policy
- Festlegung der Inhalte
- Organisatorische Strukturen
- Funktionen und Rollen
- Ergänzende Richtlinien
- Praxisbeispiel: Erläuterung der Vorgehensweise am Beispiel eines fiktiven Unternehmens

Helmut Honermann, BDG, Köln

Dienstag, 11.05.04 Aktuelle Themen

10:00 Uhr – 10:45 Uhr
Wie sicher sind unsere Netzgrenzen wirklich?
- Analyse gravierender Sicherheitsvorfälle
- Grenzen von zentralen Sicherheitslösungen
- Evolution (oder Erosion) des Perimeterschutzes
- Neueste Trends bei Bedrohungen und Schutzmaßnahmen

Detlef Weidenhammer, GAI NetConsult, Berlin

10:45 Uhr – 11:30 Uhr
Schwachstellen im LAN
- Verstärktes Auftreten von Malware-GAUs; Möglichkeiten von Innentätern
- Lehren aus den letzten Angriffen für die interne Netzstruktur und das Routing
- Netzstrukturen für firmeneigene und andere mobile Benutzer
- Benutzer- und Rechtemanagement (Identity Management)

Dr. Behrooz Moayeri, ComConsult Beratung und Planung, Aachen

12:00 Uhr – 13:00 Uhr
IDS/IPS im praktischen Einsatz
- Abgrenzung heute verwendeter Techniken
- Konfrontation mit realen Angriffen (Wurm, Exploit)
- Bewertung unterschiedlicher Erkennungstechniken
- Hinweise zur Integration in die Systemumgebung

Christian Graf, Security Consultant

14:30 Uhr – 15:15 Uhr
Sicherheit bei Webanwendungen
- Hauptangriffspunkte gegen Webanwendungen: Ergebnisse von Security Audits
- Sichere Konzeption und Programmierung bei Neuerstellung
- Wie können bestehende Webanwendungen nachträglich effizient gesichert werden?
- Einsatz von speziellen Web Application Security Gateways

Frank Breitschaft, GAI NetConsult, Berlin

15:15 Uhr – 16:00 Uhr
Rechtliche Haftungsrisiken für Netzwerk- und Webadministratoren
- Haftungsverteilung Firma/Administrator/IT-Leitung
- Haftung bei Patch- und Notfallmanagement
- Haftung bei Überwachungsdefizit
- Informationspflichten des Administrators

Ulrich Emmert, esb Rechtsanwälte, Stuttgart

16:30 Uhr – 18:00 Uhr
Diskussionsrunde mit namhaften Herstellern
- Welche Bedrohungen der IT-Sicherheit werden unter- überschätzt?
- Welche Sicherheits-Technologien sind besonders zu beachten?
- Wie wird der Umgang mit der IT-Sicherheit bei deutschen Unternehmen eingeschätzt?
- Sicherheits-Standards und Interoperabilität von Sicherheitslösungen
- Kurzvorstellung der Hersteller-Strategien
- Fragen aus dem Auditorium

Moderation: Detlef Weidenhammer, GAI NetConsult, Berlin

Mittwoch, 12.05.04 Praxis-Workshops

Workshop 1: Security Gateways zur Sicherung von Webanwendungen

- Moderierter Produktvergleich mit Live-Szenarien
- Welche Sicherheitsfeatures bieten die verschiedenen Produkte? Reicht dies aus?
- Welche Maßnahmen sind weiterhin am Zielsystem erforderlich?
- Werden auch unsichere Webanwendungen durch Vorschaltung ausreichend gesichert?
- Welcher (initiale) Konfigurationsaufwand ist erforderlich?

Frank Breitschaft, GAI NetConsult, Berlin

Workshop 2: IDS/IPS Systeme im Vergleich

- Technische Ansätze: HIDS & NIDS, IDP & IDS (inline & Sniffer Modus)
- IPS-Funktionen in Firewalls und anderen Appliances
- Gegenüberstellung kommerzieller und SNORT-basierende IPS-Lösungen
- Live-Demo

Karl-Heinz Jaeger, BDG, Köln

Workshop 3: Sicherheit in Wireless LAN: WPA in der Praxis

- Sicherheitsstandards Wi-Fi Protected Access (WPA), IEEE 802.11i und WPA2 im Überblick
- Der Preis der Sicherheit: Roaming und Durchsatz auf dem Prüfstand
- Produkte im Vergleich: Aufbau, Konfiguration und Integration in das Netzmanagement
- Migration bestehender WLAN-Sicherheitsinfrastrukturen zu WPA

Dr. Simon Hoff, ComConsult Beratung und Planung, Aachen

Workshop 4: Rechtliche Aspekte von Security Policies

- Verantwortlichkeiten für Sicherheitsrichtlinien
- Geheimhaltungspflichten / Archivierungspflichten
- Inventarisierung und Lizenzmanagement
- Beweisrecht und Dokumentation
- Rechteverwaltung / Passwortschutz und Vertretungsregeln

Ulrich Emmert, esb Rechtsanwälte, Stuttgart

Workshop 5: Vergleich Multifunktionaler Security-Gateways

- Moderierter Produktvergleich mit Liveszenarien
- Vereinte Funktionalität auf einem zentralen System (Content-Filter, Anti-Virus, SSL-Proxy, Anti-SPAM,...)
- Absicherung von Mail- und Webverkehr
- Enterprise- vs User-based-Policy (Behandlung von Ausnahmen)
- Integration in die vorhandene IT-Umgebung

Detlef Weidenhammer, GAI NetConsult, Berlin

Workshop 6: Einsatz von Smartcards mit der Windows-PKI (Windows 2003)

- Was bietet der Windows-Standard?
- Welche Erweiterungsmöglichkeiten bestehen und welche Rahmenbedingungen müssen erfüllt sein?
- Welche Anforderungen werden an die Smartcards gestellt?
- Wie lässt sich ein effektiver Betrieb umsetzen?

Alexander Zarenko und Hans Peter Mohn, ComConsult Beratung und Planung, Aachen

Donnerstag, 13.05.04 Trends

9:00 Uhr – 9:45 Uhr
Prozessorientierte IT-Sicherheit - Vorbereitung auf eine IT-Grundschutz-Zertifizierung
- Der bereinigte Netzplan als Prozessabbild
- Der effektive Weg zur Schutzbedarfskategorisierung
- Die IT-Grundschutzerhebung und ihre Tücken - Stichwort: Dokumentation
- Das GS-Tool in der Praxis: was es leistet und was nicht

Hans Peter Mohn, ComConsult Beratung und Planung, Aachen

10:00 Uhr – 11:00 Uhr
CERT - Aufgaben und Strategien
- Dienstleistungen eines Computer-Notfallteams
- CERT-Advisories: Datenschutz vs. „full disclosure"?
- Nationale und internationale Entwicklung
- CERT: Make or Buy?

Stefan Kelm, Sercorvo, Karlsruhe

11:30 Uhr – 12:30 Uhr
Grundlagen eines effizienten Patch-Managements
- Warum rechtzeitiges Patchen so wichtig ist. Einige Beispiele
- Beschaffung von Informationen zu Schwachstellen und Patches
- Planung und Durchführung von Patchinstallationen
- Überblick zu unterstützenden Tools

Björn Fröbe, GAI NetConsult, Berlin

13:45 Uhr – 14:30 Uhr
PGP E-Mail-Verschlüsselungsproxies: Hopp oder Topp?
- Wie realisiert man einen Verschlüsselungsproxy
- Integration in die bestehende E-Mail-Infra-Struktur
- Verschlüsselung an Empfänger ohne Schlüssel
- Vor- und Nachteile des Konzepts; Produktvergleiche

Prof. Dr. Rainer W. Gerling, Max-Planck-Gesellschaft, München

14:30 Uhr – 15:15 Uhr
Mobilität mit Risiken
- Problematik der Vielfalt mobiler Geräte (Handy, PDA, Laptop)
- Bedrohungsszenarien drahtloser Medien (WLAN, Bluetooth, USB, IrDA)
- Aufbau eines „sicheren" Clients
- Organisatorische Maßnahmen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung, Aachen

15:15 Uhr – 16:00 Uhr
Sicherheit für XML Web Services
- Web Services - eine Kurzeinführung
- Besondere Sicherheitsrisiken
- Aktuelle Standards (WS-Security, SAML, XML DSig, XML Encryption)
- Sicherheitsarchitekturen (serverbasierte und gatewaybasierte)

Dr. Gerald Brose, Xtradyne Techn.

Änderungen im Programm behält sich der Veranstalter vor!

Zweitthema

Übertragung von SIP über Firewalls

Fortsetzung von Seite 1

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Zudem arbeiten viele Firewalls mit Network Address Translation (NAT), wobei nach außen nur eine oder wenige Adressen sichtbar sind, während im inneren Netz z. B. private Adressen nach RFC 1918 verwendet werden. Die Lokalisierung von Benutzern im internen Netz wäre in einem solchen Fall für einen Anrufer von außen nicht ohne Weiteres möglich.
Um die Lösungen für diese Probleme zu verstehen, muss man sich zunächst damit vertraut machen, wie SIP arbeitet.

SIP: ein kurzer Abriss

Das von der Internet Engineering Task Force (IETF) standardisierte Session Initiation Protocol (SIP) ist ein Peer-to-Peer-Signalisierungsprotokoll. SIP wird zusammen mit dem Session Description Protocol (SDP) gemäß RFC 2327 eingesetzt. SDP dient der Beschreibung der notwendigen Parameter für die Teilnahme an einer Multimedia-Session, z. B. des genutzten Mediums, der genutzten Kodierung, der Abtastrate, der IP-Adresse und Portnummer, des Session-Namens etc. SDP ist trotz der Bezeichnung eher ein Datenformat und weniger ein Protokoll.
SIP ist ein Ende-zu-Ende-Client-Server-Signalisierungsprotokoll einschließlich Verbindungsauf- und -abbau und Änderungen zwecks Unterstützung der Lokalisierung von mobilen Benutzern. Eine SIP-Nachricht kann neben der Session-Beschreibung auch kurze Messages sowie Bildinformationen in Formaten wie JPEG (Joint Photographic Exper Group) beinhalten.

Folgende Instanzen sind im SIP-Standard vorgesehen:

- UA: User Agent, eingebettet als Software oder Hardware in die Endgeräte, zuständig für
  - UA Client (Initiierung von Anrufen)
  - UA Server (Entgegennahme eingehen der Anrufe)
- SIP Registrar: Diese Instanz akzeptiert Registrierungsanfragen der Benutzer und aktualisiert die Informationen eines Location Servers über die Position der Benutzer (analog zum HLR – Home Location Registry - bei GSM, Global System for Mobile Communication)
- SIP Proxy Server: Diese Instanz, auch Signaling Relay genannt, agiert als Client und Server und nimmt keine Session-Status-Informationen auf, sondern arbeitet im Transaktionsmodus
- SIP Redirect Server: Diese Instanz leitet den rufenden Kommunikationspartner zu anderen Servern um

SIP verwendet global erreichbare Adressen für Benutzer, ähnlich wie E-Mail-Adressen. Die UA-Server der Endgeräte melden diese Adressen beim Registrar an. Der dazu verwendete Befehl heißt SIP REGISTER. UA-Clients verwenden diese Adressen, um Sessions aufzubauen.
Das Format für die Adressen ist eine Art URL (Unified Resource Locator), wie z.B.

Seminar zum Thema

Sicherheits-Lösungen: Von den Einzelbausteinen zur integrierten Lösung Seminar

03.05. - 07.05.04 in Zürich

24.05. - 28.05.04 in Köln

05.07. - 09.07.04 in Bonn

11.10. - 15.10.04 in Bonn

Dieses Seminar vermittelt, aus welchen Bausteinen eine effiziente Sicherheits-Lösung aufgebaut wird, welche Bausteine unverzichtbar sind und wie diese Bausteine konfiguriert werden. Jeder einzelne Baustein wird detailliert erklärt und in seinen Potenzialen beschrieben. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.
Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans Peter Mohn
Einzelpreis: € 2.290,- zzgl. MwSt.

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

sip:user@comconsult.com.
Die bei SIP verwendeten Befehle heißen SIP-Methoden und umfassen die Methoden INVITE, ACK, BYE, CANCEL, OPTIONS und REGISTER. SIP Response Codes sind HTTP-ähnlich und bestehen aus einer Nummer, gefolgt von einer verbalen Erklärung des Response Codes.

Der SIP Registrar ist dafür zuständig, die Anmeldungen der User Agents entgegenzunehmen und die entsprechenden Informationen über die Lokation des Benutzers zu speichern. Dies erfolgt in der Regel in Form der Übergabe der Information an einen Location Server. Dieser Ablauf ist in der Abbildung 1 wiedergegeben.
Der User Agent (UA) verwendet die SIP-Methode REGISTER, um die eigene SIP-Adresse sowie die IP-Adresse, über die der UA erreichbar ist, dem Registrar mitzuteilen. Diese Informationen werden vom Registrar an den Location Server übergeben. So ist der Location Server in der Lage, die zu einer SIP-Adresse zugeordnete IP-Adresse mitzuteilen.

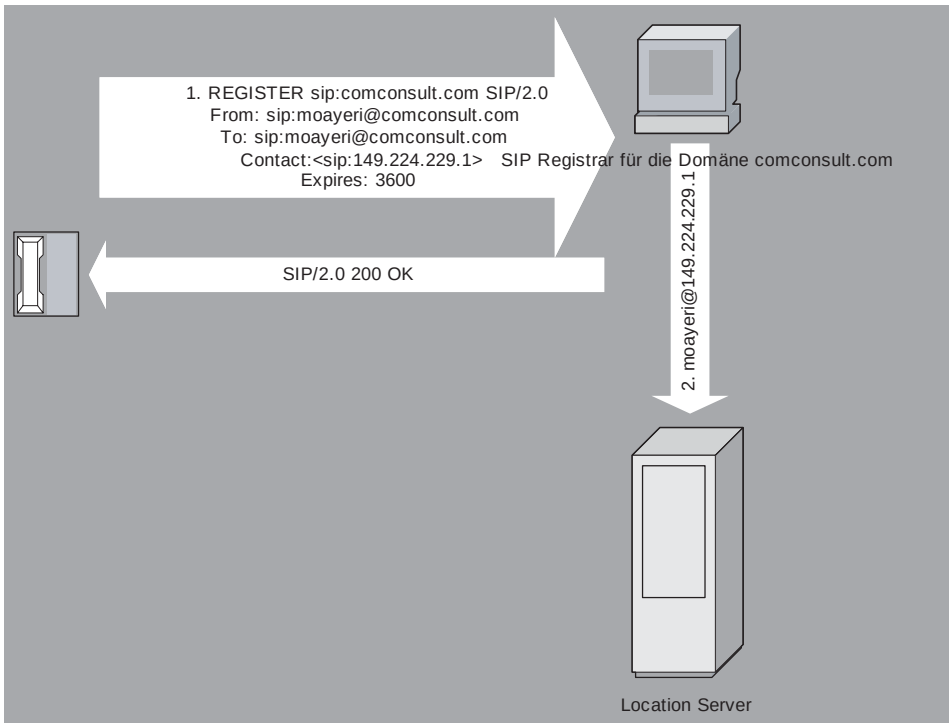


Abbildung 1: Registrierung bei SIP

SIP Proxy

Die Antwort auf die Probleme mit dynamischen Ports für Peer-to-Peer-Kommunikation und die Auffindung von hinter Firewalls „versteckten“ Benutzern ist der SIP Proxy, der im SIP-Standard selbst vorgesehen ist.
SIP Proxy Server übernehmen wichtige Vermittlungsfunktionen bei der Initialisierung von Sessions mit Hilfe von SIP. Bei eingehenden Rufen stellt z. B. ein SIP Proxy Server die zentrale Anlaufstelle für eine administrative Domäne dar, ungefähr vergleichbar mit einem zentralen Mail-Server. Eingehende SIP-Einladungen werden z. B. an den Eingangs-Proxy-Server der administrativen Domäne gerichtet, wie aus der Abbildung 2 hervorgeht.
Der anrufende Kommunikationspartner bringt zunächst über das Domain Name System (DNS) die IP-Adresse des Eingang-SIP-Proxy-Servers einer Organisation in Erfahrung und sendet die SIP-Einladung an diesen Proxy-Server. Die SIP-Einladung beinhaltet die SIP-Adresse des anzurufenden Kommunikationspartners und, wie bei jeder Signalisierung üblich, eine Identifikationsnummer für den Anruf. Der Proxy-Server greift ggf. auf einen Location Server zu, um die passende IP-Adresse zu der SIP-Adresse in der Einladung herauszufinden. An diese IP-Adresse wird die SIP-Einladung weitergeleitet. Der so angerufene

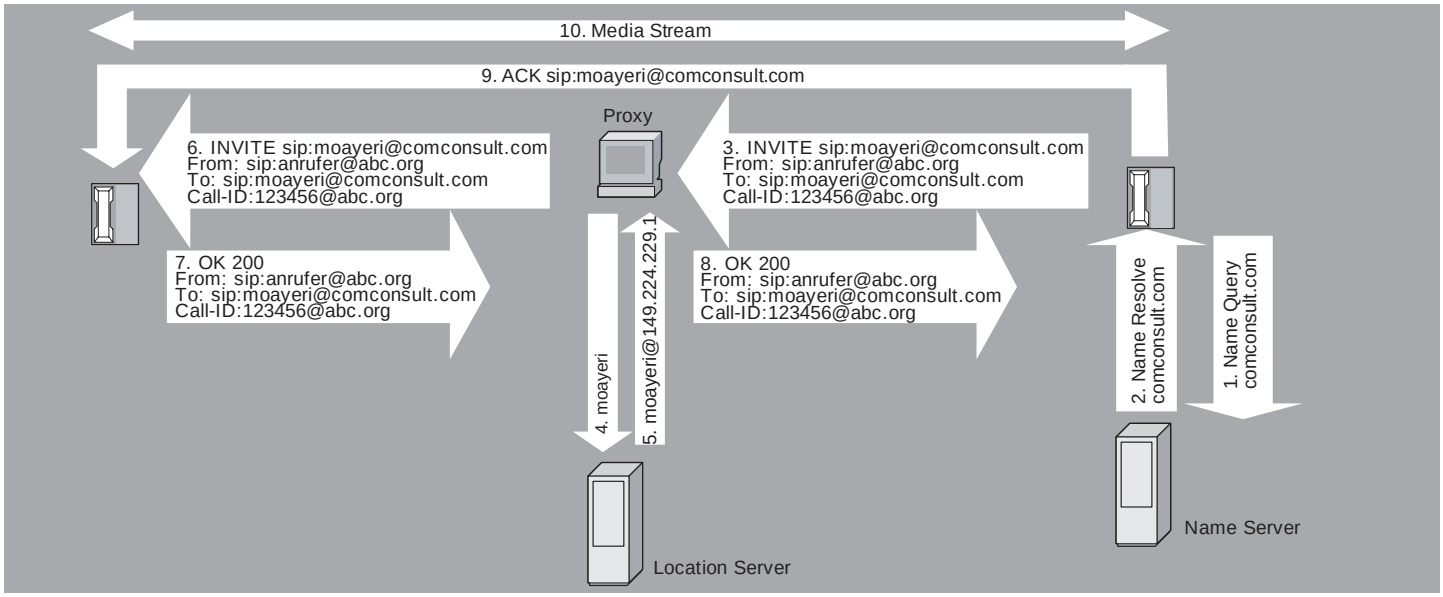


Abbildung 2: Annahme einer SIP-Einladung

Kommunikationspartner kann den Ruf (die SIP-Einladung) entgegennehmen. Diese Bestätigung, die anhand der enthaltenen Identifikationsnummer der ursprünglichen Einladung zugeordnet werden kann, wird vom Proxy-Server an den anrufenden Kommunikationspartner weitergeleitet.
An dieser Stelle endet die Arbeit des Proxy-Servers. Man spricht von einer Transaktion, die von diesem Server abgewickelt wurde. Auf dem Proxy-Server erfolgt keine Buchführung über den Status der Session. Mit dieser Transaktion vermittelt der Proxy-Server zwischen den beiden Kommunikationspartnern. Nach dem Abschluss dieser Transaktion können die beiden Kommunikationspartner direkt miteinander kommunizieren, Informationen austauschen (z. B. kodierte Sprache) und die Session abbauen, ohne dass der Proxy-Server dies mitbekommt. Dieser Sachverhalt ist in der Abbildung 3 dargestellt.
In diesem Beispiel erfolgt der Session-Aufbau mithilfe einer vom Proxy-Server durchgeführten Transaktion, nicht jedoch der Session-Abbau, der durch direkte Signalisierung zwischen den beiden Kommunikationspartnern durchgeführt wird.
Das oben dargestellte Beispiel verdeutlicht die Funktion eines Eingang-Proxy-Servers. Ein SIP-Proxy-Server kann jedoch auch als Ausgang-Proxy-Server zum Einsatz kommen, der z. B. Firewalling-Funktionen übernimmt. Diese Situation ist in der Abbildung 4 dargestellt.
in diesem Beispiel wendet sich der anrufende Partner an einen Proxy-Server, um mit einem externen Kommunikationspartner eine Session aufzubauen. Der Proxy-Server übernimmt Firewalling-Funktionen wie z. B. Prüfung der Berechtigung des Anrufers für externe Kommunikation. Die zugehörige SIP-Einladung kann nach erfolgter Prüfung an einen anderen Proxy-Server weitergeleitet werden. Dies ist in einer größeren Umgebung mit einer Vielzahl von administrativen Domänen sinnvoll und für eine in einer solchen Umgebung unerlässliche hierarchische Anordnung erforderlich. Die SIP-Einladung kann somit eine Kette von Proxy-Servern durchlaufen, bevor sie am Ziel ankommt. Ein weiterer Proxy-Server kann z. B. dafür zuständig sein, für Anrufe in das konventionelle PSTN (Public Switched Telephone Network) den günstigsten Gateway zu bestimmen und den Anruf an diesen zu signalisieren.
Auch in diesem Beispiel arbeiten die SIP-Proxy-Server transaktionsorientiert und vermitteln zwar die Session, sind jedoch nach dem Aufbau der Session nicht mehr in den weiteren Ablauf integriert. Dieser weitere Ablauf der Session findet in diesem Fall zwischen dem anrufenden Kommunikationspartner und dem Gateway statt, der den Übergang zwischen der SIP-Umgebung und dem PSTN bereitstellt.

SIP-bewusste Firewall

Nun muss auch die Multimedia-Session (z. B. das Telefongespräch) über Firewalls abgewickelt werden. Für jede Session müssen die entsprechenden Ports geöffnet und (vor allem) nach Abbau der Session wieder geschlossen werden. Dies kann nur eine SIP-bewusste Firewall bewerkstelligen, welche Ports nach Bedarf öffnet und schließt.

Eine solche Firewall muss ein weiteres Problem lösen, das durch NAT entsteht: die im SIP-Header enthaltene IP-Adresse ist nicht gleich der Adresse, die der Kommunikationspartner verwenden muss, um die Session aufzubauen. Die Firewall muss nicht nur den IP- und den UDP-Header, sondern Inhalte von SIP-Paketen ändern. Die SIP-bewusste Firewall ist ein SIP Proxy Server, der die Adressen und Ports entsprechend anpasst.

Die Firewall muss mit dem Location Server im internen Netz zusammenarbeiten, um einen Benutzer zu finden, da sämtlicher eingehender SIP-Verkehr an Port 5060 der selben IP-Adresse (externe Adresse der Firewall) gerichtet sein kann.

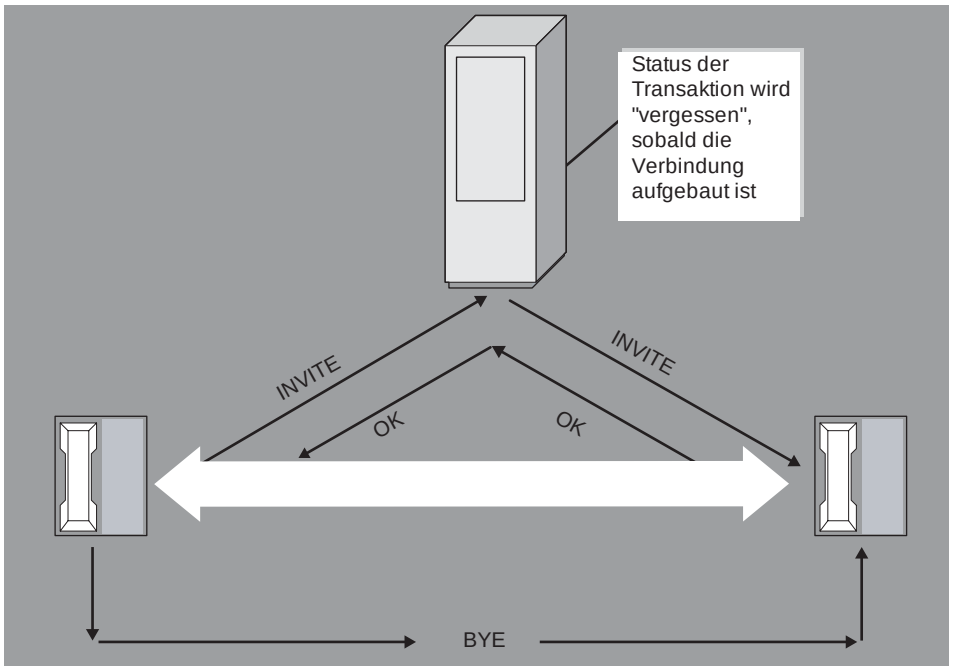


Abbildung 3: SIP-Server arbeiten transaktionsorientiert

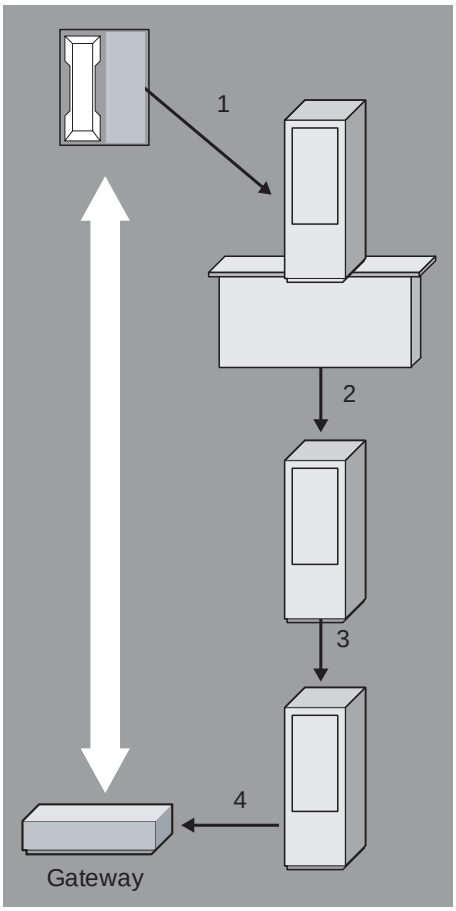


Abbildung 4: Kaskadierung von SIP-Proxy-Servern

Übertragung von SIP über Firewalls

Der Location Server kann separat oder in die Firewall integriert sein. Die Firewall fungiert in diesem Fall als SIP Registrar. Die Firewall muss den internen SIP-Benutzern die Möglichkeit bieten, sich zu registrieren. Die Registrierungen müssen nach Ablauf eines Timeout-Werts gelöscht werden, weil keine Gewähr dafür besteht, dass sich alle Endgeräte ordnungsgemäß abmelden.
Aus der Sicht der Informationssicherheit muss der Firewall-Administrator jederzeit in der Lage sein zu überwachen, welche Ports geöffnet sind. Bestimmte MIME-Typen, die Bestandteil von SIP Messages sein können, müssen gesperrt werden können. Der SIP Registrar muss eine Authentifizierung über Digest Access Authentication wie bei HTTP unterstützen, damit nur vertrauenswürdige Endgeräte bzw. Benutzer sich registrieren können.

Eingehende SIP-Session

Im folgenden betrachten wir eine eingehende SIP-Session durch eine SIP-bewusste Firewall, wie in der Abbildung 5 dargestellt. Im dargestellten Beispiel verbindet eine Firewall das interne Netz (Adressbereich 149.224.0.0/16) mit der Außenwelt. Die externe Adresse der Firewall ist 210.1.1.1. Sämtliche externe Kommunikation erfolgt über die letztgenannte Adresse.
Vom externen SIP-Endgerät mit der Adresse 200.1.1.1 soll eine Session mit dem Benutzer sip:moayeri@comconsult.com aufgebaut werden, der sich zurzeit über das interne SIP-Endgerät mit der Adresse 149.224.229.1 beim SIP Registrar registriert hat. Die letztere Adresse ist jedoch nach außen nicht sichtbar.
Nach der Namensauflösung für comconsult.com sendet das externe Endgerät eine SIP-INVITE-Meldung an den Eingangs-SIP-Proxy-Server der Domäne comconsult.com. In dieser INVITE-Nachricht wird u. a. mitgeteilt, welcher Domäne der Anrufende angehört, wen in der Domäne comconsult.com er anzurufen versucht und über welchen Port sein Endgerät Audio-Informationen empfangen wird (in diesem Fall Port 15000).
Alle Pakete an Port 5060, die durch die SIP-bewusste Firewall gehen sollen oder an die Firewall selbst gerichtet sind, werden von dieser aufgefangen. Header und Body des Paketes werden untersucht. Der Body des SIP-Paketes enthält möglicherweise SDP-Information über Informationsströme, die der Sender empfangen möchte, und die IP-Adressen und Ports. Einige dieser Informationen werden von der Firewall gespeichert (Stateful Transaction). Der Proxy Server bringt durch eine Kommunikation mit dem Location Server in Erfahrung, über welches interne Endgerät der Benutzer moayeri@comconsult.com erreichbar ist. Das Paket wird weitergeleitet, und zwar an das Endgerät, von dem aus der Benutzer sich beim Registrar registriert hat.
Von einem Pool von Ports, die für SIP-initiierte Sessions reserviert sind, wird auf der externen Seite ein Port für die Kommunikation belegt. Angaben zu IP-Adresse und Ports jedes SIP-Paketes werden von der Firewall neu geschrieben. Auch der vom

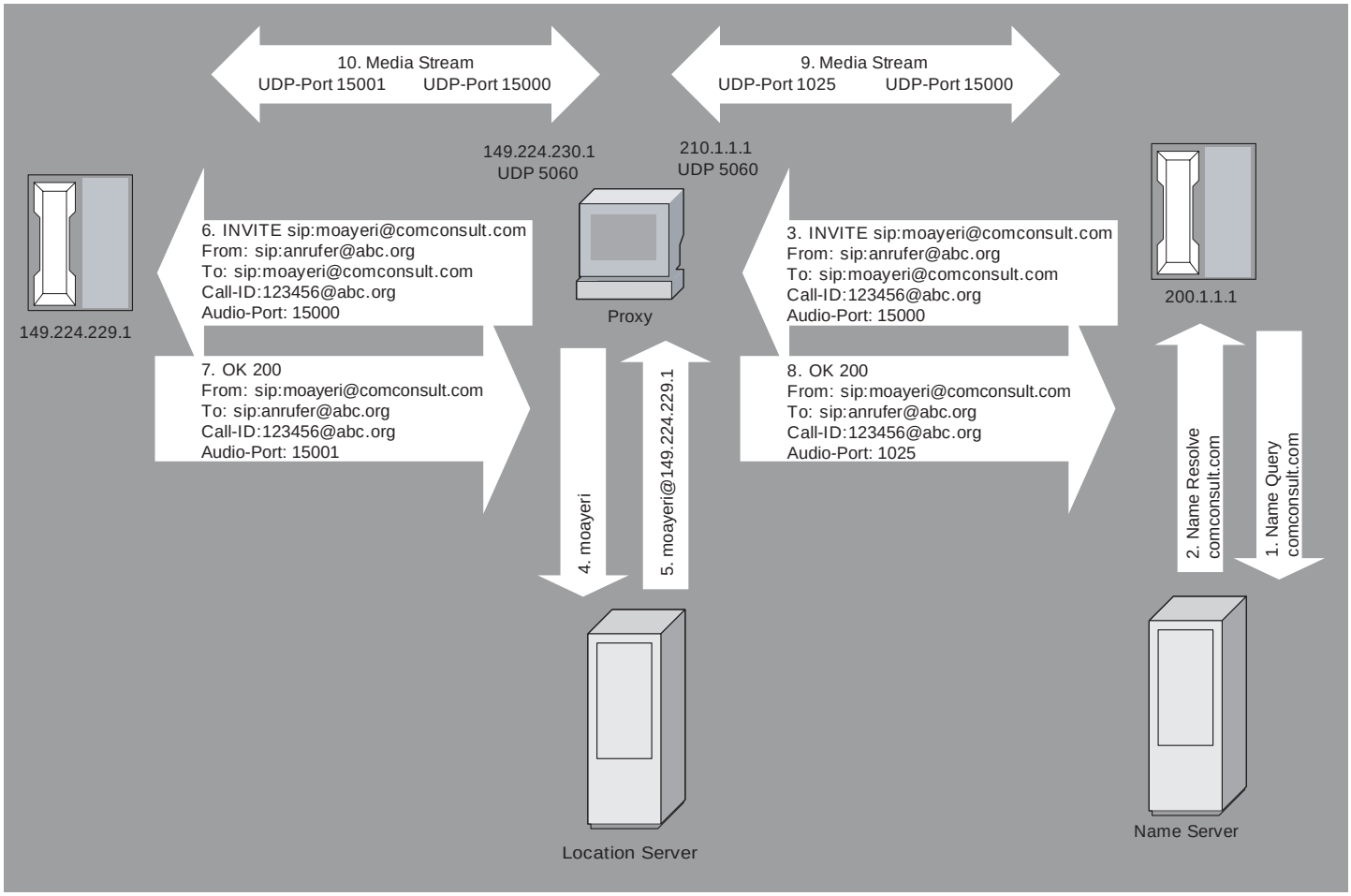


Abbildung 5: Eingehende SIP-Session durch SIP-bewusste Firewall

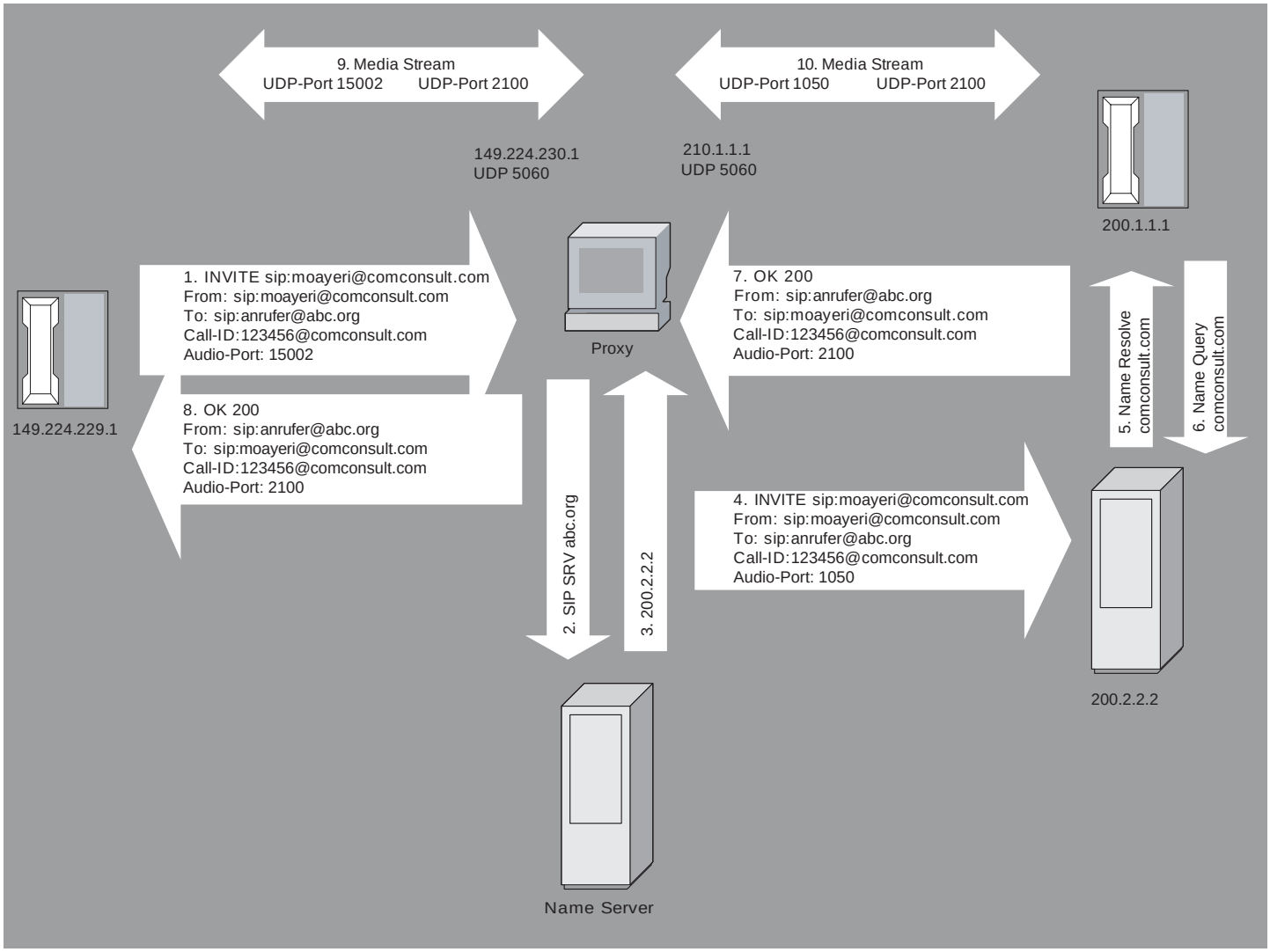


Abbildung 6: Ausgehende SIP-Session durch SIP-bewusste Firewall

Client ausgefüllte SIP-„via“-Header wird ersetzt.
Eine temporäre Regel zum Durchlassen des Informationsstroms wird aufgestellt. Alle zu diesem Informationsstrom gehörenden Pakete werden aufgefangen und modifiziert. Nach der etwas aufwändigeren Phase des Verbindungsaufbaus beschränkt sich die Rolle der Firewall darin, die Adressinformationen in den Paketen umzuschreiben. Somit können SIP-bewusste Firewalls die RTP-Pakete, die eigentlichen zeitkritischen Informationen einer VoIP-Session, relativ schnell weiterleiten. Der SIP-Firewall-Hersteller Ingate aus Schweden gibt zum Beispiel an, dass nach 0,15 Sekunden, die in der Firewall für den Verbindungsaufbau gebraucht werden, die RTP-Pakete durch die Firewall lediglich 0,08 bzw. 0,19 ms lang verzögert werden (bei 100 bzw. 10 Mbit/s).

Bei Abbau der Session wird die Firewall-Regel entfernt.

Ausgehende SIP-Session

Eine ausgehende SIP-Session ist in der Abbildung 6 dargestellt.

Auch hier werden alle Pakete an Port 5060, die durch die Firewall gehen sollen oder an die Firewall selbst gerichtet sind, von dieser aufgefangen, und Header und Body des Paketes werden untersucht. Mehrere Header wie via- und routing-Header sowie Teile des Body werden von der Firewall ersetzt und/oder gespeichert. Die Vergabe der Portnummer aus dem Pool von Ports, die für SIP reserviert sind, sowie die Aufstellung einer temporären Firewall-Regel erfolgt analog zur eingehenden Session.

Das Paket wird weitergeleitet, und zwar ggf. an einen externen SIP Relay. Wenn kein externer SIP Relay definiert ist, versucht die Firewall, einen SIP-Server zu finden, indem das DNS für die Auffindung eines SRV-Eintrages (analog zu einem Mail-SRV-Eintrag im DNS) bemüht wird. Wenn kein SRV-Eintrag vorhanden ist, wird das Paket an die Zieldomäne selbst gesendet.

Was tun, wenn die Firewall SIP nicht kennt?

In fast allen Unternehmen gibt es bereits Firewall-Systeme, die das interne Netz mit unsicheren Netzen wie dem Internet verbinden und zugleich vor Angriffen und Risiken schützen, die von den unsicheren Netzen ausgehen. SIP ist ein relativ junges Protokoll. Obwohl die meisten Fire-

wall-Hersteller SIP-Unterstützung auf ihre Fahnen geschrieben haben, ist eine solche umfassende Unterstützung wie in diesem Beitrag dargestellt noch selten realisiert. Was sollten Unternehmen tun, die nicht SIP-bewusste Firewalls einsetzen, zugleich aber SIP-Kommunikation auch extern implementieren müssen?
Eine mögliche Lösung ist in der Abbildung 7 dargestellt.

Im dargestellten Beispiel ist das rechts dargestellte LAN mit SIP-Telefonen über eine Firewall ohne SIP-Kenntnis mit dem Internet verbunden. Im Internet gibt es bereits viele Gateways zum öffentlichen Telefonnetz (Public Switched Telephone Network, PSTN).

Die Firewall muss so konfiguriert werden, dass sämtliche SIP-Kommunikation sowie sämtlicher UDP-Verkehr im denkbaren Portbereich für Audiokommunikation über einen SIP-Proxy-Server geleitet wird, der an die Demilitarisierte Zone (DMZ) angeschlossen ist. Will zum Beispiel ein internes SIP-Endgerät eine ausgehende Session aufbauen, sendet es eine SIP-INVITE-Nachricht. Die Firewall ist so eingestellt, dass diese Nachricht an den SIP-Proxy-Server umgeleitet wird. Dieser verfährt wie im SIP-Standard vorgesehen, und leitet über die Firewall die INVITE-Nachricht weiter nach außen.

Eine weitere Firewall-Regel kann z. B. vorgeben, dass die INVITE-Nachricht an den SIP-Proxy-Server eines Providers weitergeleitet wird. Dieser kann eine Relay-Funktion zu einem PSTN-Gateway ausüben.
Die Audio-Session wird über UDP-Ports abgewickelt. Die Firewall kann so eingerichtet sein, dass unbekannte UDP-Pakete von innen nach außen bzw. von außen nach innen an den SIP-Proxy-Server weitergeleitet werden, der zudem eine RTP-Proxy-Funktion wahrnimmt.

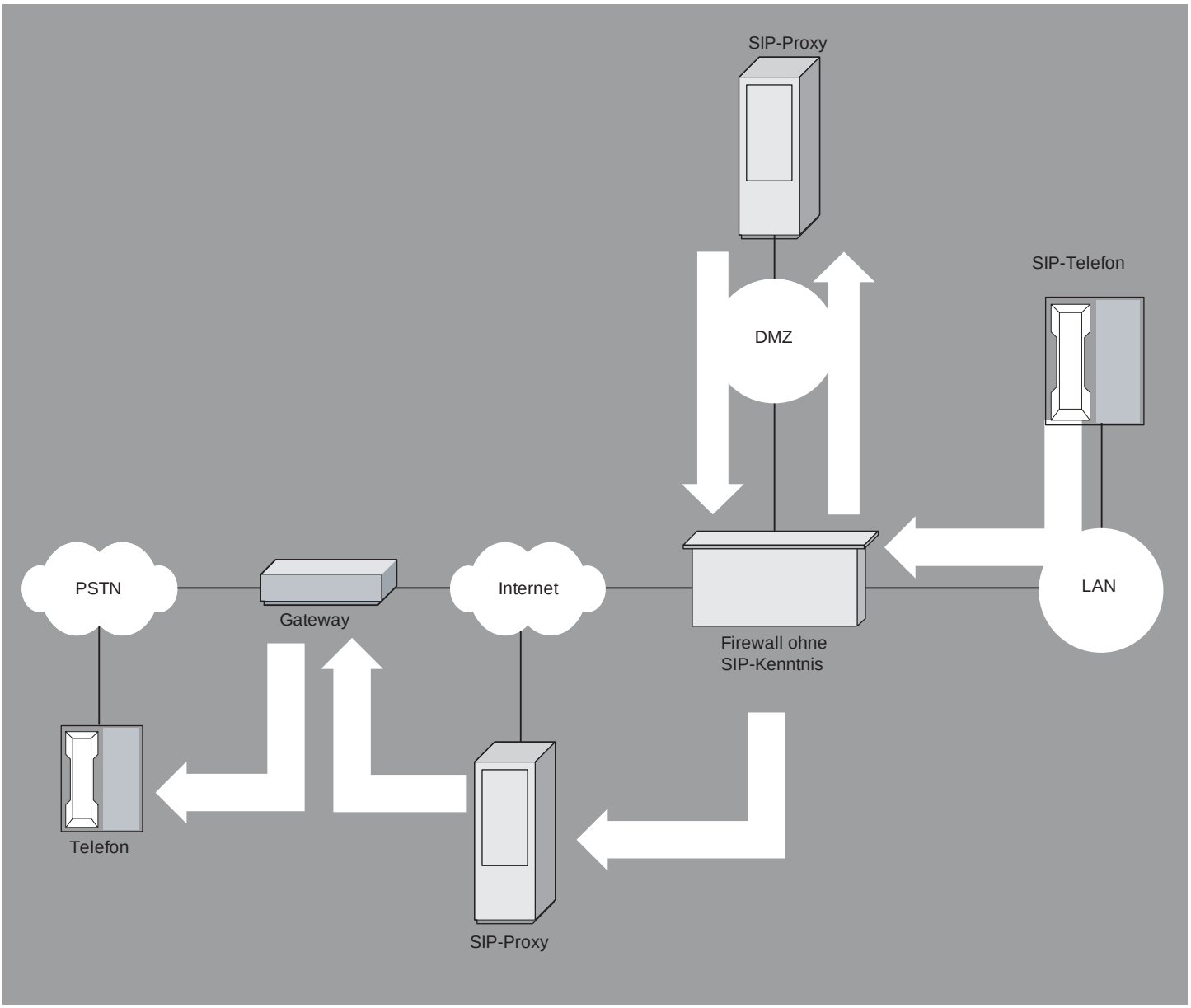


Abbildung 7: SIP-unbewusste Firewall im Kombination mit SIP Proxy

Übertragung von SIP über Firewalls

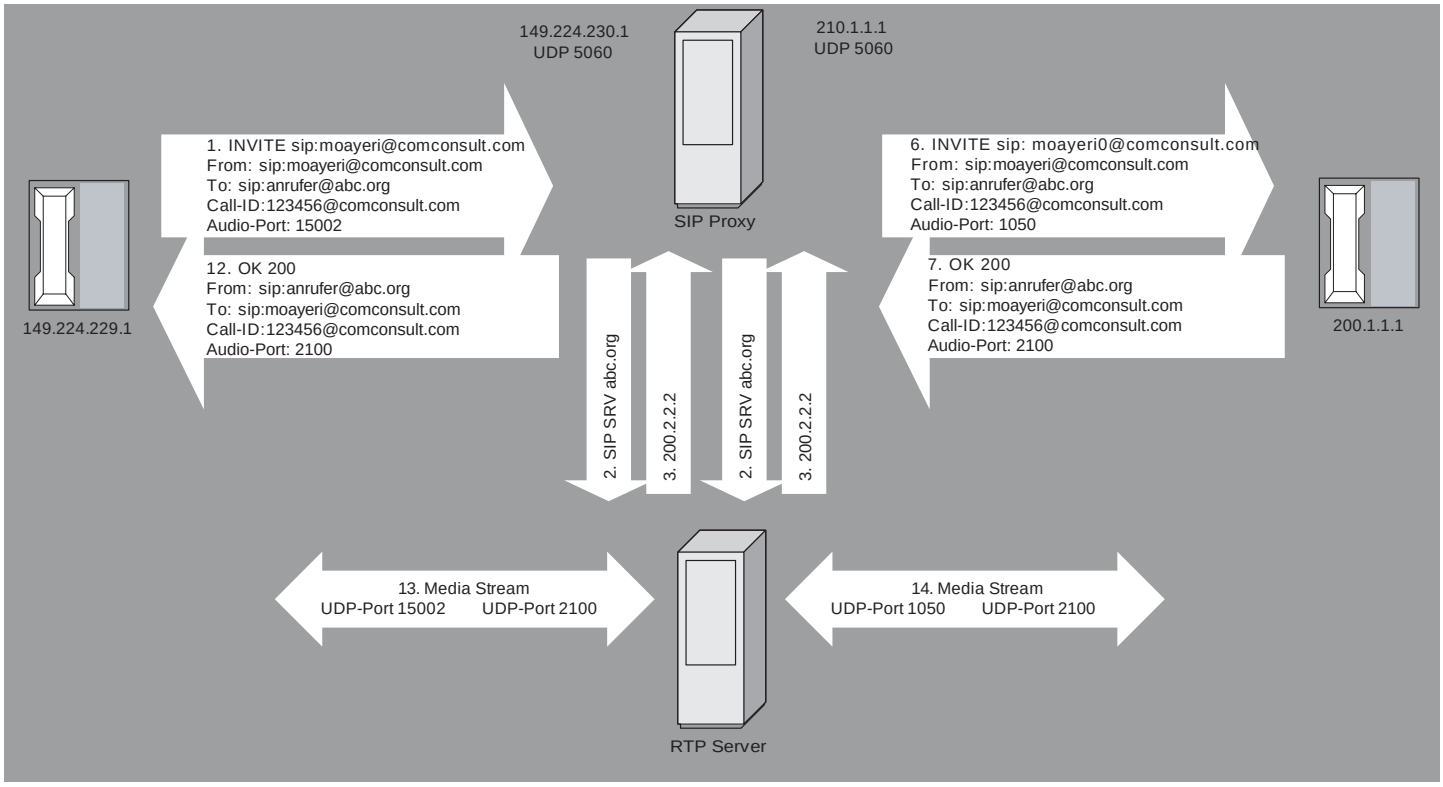


Abbildung 8: Trennung von SIP und RTP Proxy

Trennung des SIP vom RTP Proxy

Einige Firewall-Hersteller bieten bereits eine Kombination aus SIP und RTP Proxy. Es ist jedoch denkbar, dass diese Lösung nicht in ausreichendem Maße nach oben skaliert. Vorhandene Standards ermöglichen eine Trennung der beiden Funktionen. Dieser Ansatz geht aus der Abbildung 8 hervor.

Bei diesem Ansatz kontrolliert der SIP-Proxy-Server die RTP-Proxy-Instanz über das Media Gateway Control Protocol (MGCP).

Eine SIP-INVITE-Nachricht wird vom internen SIP-Client 149.224.229.1 in Richtung externes Netz gesendet. Der SIP-Proxy-Server kopiert die Session-Merkmale aus dem SIP-Paket in einen MGCP-Befehl und veranlasst die RTP-Proxy-Instanz, eine Verbindung mit dem internen SIP Agent aufzubauen. Noch ist diese Verbindung inaktiv.

Nachdem die RTP-Proxy-Instanz die Verbindung mit dem internen Agent aufgebaut hat, teilt sie in einer Bestätigung die Einzelheiten der Verbindung dem SIP-Proxy-Server mit. Der SIP-Proxy-Server veranasst den Aufbau einer weiteren Verbindung, diesmal zwischen der RTP-Proxy-Instanz und dem Ziel-Agenten im externen Netz. Außerdem wird der RTP-Proxy-Instanz vorgegeben, dass sie eine Relay-Funktion zwischen den beiden Verbindungen nach außen und innen wahrnehmen soll.

Modifikationen der Verbindungen zum Beispiel bei Annahme einer Session durch einen Zielagenten werden ebenfalls vom SIP-Proxy-Server an die RTP-Proxy-Instanz signalisiert.

Weitere Ansätze

Ein anderer Ansatz besteht darin, SIP über einen sicheren Kanal gemäß Transport Layer Security (TLS) abzuwickeln. Dabei muss ein Identifikationsmerkmal für die Hosts verwendet werden, das sich nicht an der IP-Adresse orientiert. TLS-Kanäle können nämlich über NAT-Firewalls aufgebaut werden, weshalb die IP-Adresse nicht als Identifikationsmerkmal der Endgeräte verwendet werden kann.

Einen anderen Ansatz bietet das Simple Traversal of UDP Through NAT (STUN2). Dabei handelt es sich um ein Protokoll, das den Applikationen die Entdeckung von NAT-Instanzen auf dem Pfad zwischen den beiden Endpunkten der Kommunikation ermöglicht. So kann beispielsweise ein SIP-Endgerät im inneren Netz herausfinden, über welche IP-Adresse es im externen Netz erreichbar ist.

NAT-bewusste Endgeräte, welche die durch NAT verwendeten IP-Adressen „entdecken“, haben jedoch den Nachteil, dass SIP-Applikationen geändert werden müssen. Außerdem gibt es verschiedene NAT-Varianten, was die Komplexität noch weiter erhöht.

Daher geht der Autor davon aus, dass die Lösung mit SIP-Proxy-Servern, die in den Firewalls implementiert werden, die am weitesten verbreitete Lösung sein wird.

Anforderungen an die Firewalls

Eine SIP-bewusste Firewall muss folgende Funktionen unterstützen:

- SIP Registrar Server für die Entgegennahme von REGISTER Requests der internen Clients
- SIP Proxy Server für Adressauflösung für jeden SIP-Request von außen nach innen und von innen nach außen
- Stateful oder stateless Transaktion, je nach SIP-Request
- Parallel forking (gleichzeitige Weiterleitung eines Requests zu mehreren Zie-

len, zum Beispiel im Falle von Konferenzen sinnvoll)
- Digest Authentication: sinnvoll für die Authentifizierung von internen Clients
- Session Timer für den Abbau nicht genutzter Sessions
- Unterstützung für DNS SRV Record, damit analog zu SMTP Eingangs-Proxy-Server anderer Domänen durch Zugriff auf DNS lokalisiert werden können
- TLS für verschlüsselte SIP-Signalisierung (SIP Messages werden auch für Short Messages verwendet, die somit auch verschlüsselt werden können)
- Skalierbarkeit hinsichtlich der Zahl der internen SIP Clients
- Performance hinsichtlich der Zahl der parallelen Sessions

Fazit

Immer mehr Firewall-Hersteller unterstützen SIP. Dabei ist zu achten, dass die implementierte Lösung folgende Probleme löst:
- Lokalisierung interner Benutzer durch externe Kommunikationspartner trotz Network Address Translation (NAT)
- Kontrolle über dynamisch eröffnete Ports für Multimedia-Kommunikation
- Modifikation der SIP-Pakete bei Anwendung von NAT

Die in diesem Beitrag aufgeführten Anforderungen an Firewalls müssen zur Lösung dieser Probleme erfüllt werden.

SIP-Firewalls für den Heimgebrauch

Neben dem PSTN entwickelt sich das Internet zum Medium für Telefonie. Insbesondere bei nicht sehr hohen Anforderungen an die Sprachqualität und die Verfügbarkeit, dafür aber hohen Anforderungen an die Wirtschaftlichkeit, können sich künftig VoIP-Angebote der Provider zu durchaus interessanten Varianten für die öffentliche Telekommunikation entwickeln.

Bereits viele Haushalte in den USA und den skandinavischen Ländern nutzen Telefonanschlüsse über IP. Zum Beispiel kann ein Kabelmodem neben den Ports für den Fernseher und den PC auch einen analogen Port für das Telefon beinhalten. Eine andere Variante wäre die Nutzung eines SIP-Telefons zuhause. Das SIP-Telefon kann entweder ein dediziertes Endgerät sein (mit Preisen unter 100 Euro ist künftig zu rechnen) oder auf PC-Softphones basieren. Insbesondere im letzteren Fall ist der Schutz vor Angriffen wichtig. Sicherheitsbewusste Anwender schützen ihre PC durch Firewalls vor Angriffen aus dem Internet. Solche Firewalls müssen SIP-bewusst arbeiten, wenn auf dem PC auch noch ein SIP-Telefon als Softphone laufen soll.
Eine mögliche Konstellation geht aus der Abbildung 9 hervor.
Wenn z. B. das rechts unten dargestellte SIP-Telefon ein Mobiltelefon im GSM-Netz anrufen will, sendet es eine SIP-Invite-Nachricht ins Internet. Diese Nachricht muss die Firewall passieren. Die SIP-bewusste Firewall kann so eingestellt sein, dass ausgehende SIP-Requests an den SIP Proxy Server des Providers weiter geleitet werden. Diese kann den Gateway zum PSTN lokalisieren. Darüber wird der Anruf zum Ziel geroutet.
In einem anderen Home Office (links oben) verläuft der Anruf zum ersten Home-Office ähnlich, mit dem Unterschied, dass der Anruf zur Firewall des ersten Home Office geroutet wird. Trotz Verwendung privater Adressen hinter der Firewall ist diese in der Lage, das SIP-Telefon zu finden und den Anruf dorthin zu signalisieren.

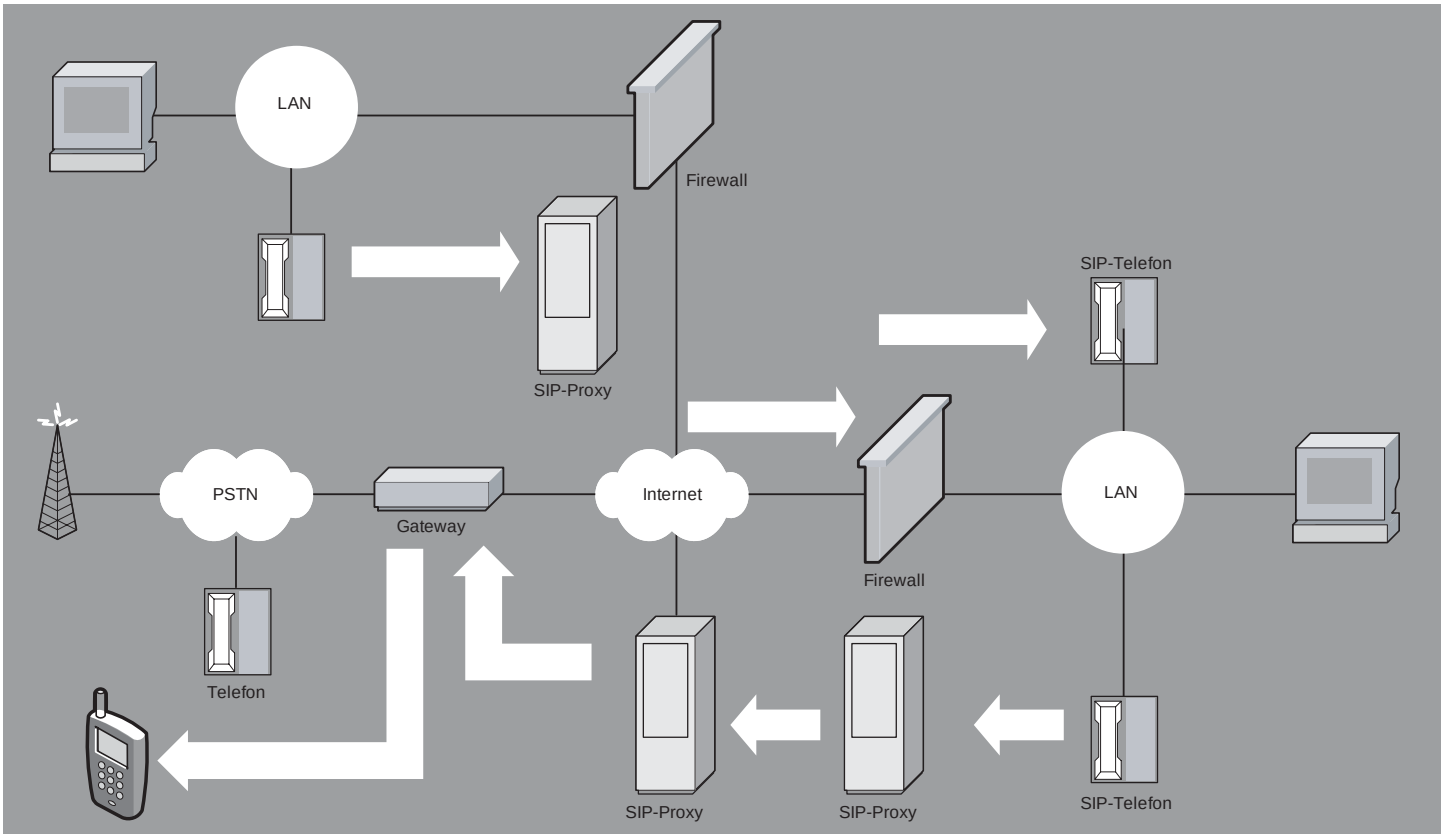


Abbildung 9: SIP-bewusste Firewall für Home Office

Neues Seminar

IT-Sicherheitsmanagement in der Praxis

Vom 28. bis 30. Juni 2004 veranstaltet die ComConsult Akademie erstmalig ihr neues Seminar „IT-Sicherheitsmanagemenet in der Praxis“ im Jolly Hotel in Köln.

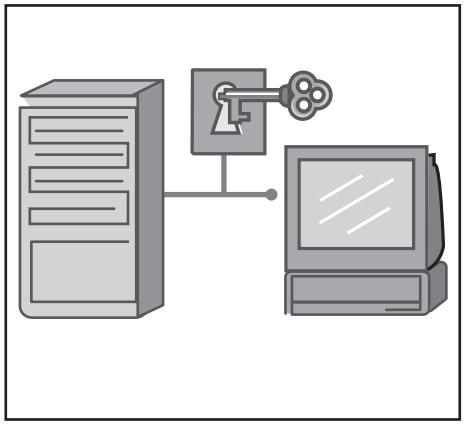
Effektive IT-Sicherheit entsteht nicht durch technische Einzellösungen. Notwenig ist ein vollständiger, umfassender Maßnahmenkatalog quer durch alle technischen Aspekte des IT-Einsatzes. Dieser entfaltet aber nur dann seine volle Stärke, wenn er möglichst nahtlos in die Umgebung, also auch in die Prozesse eingebettet wird.

Lange fehlten hier anerkannte Methoden und Standards. Für jedes Unternehmen entsteht so das Problem, die Qualität und Vollständigkeit seiner Lösung zu prüfen und ggf. auch nachzuweisen. Mittlerweile sind solche Standards durch das BSI-Grundschutzhandbuch und den BS799 etabliert. Diese weisen mit Anforderungs- und Maßnahmenkatalogen unterschiedlicher Detailtiefe Wege zu (zertifizierbarer) Sicherheitsqualität.

Ein Standard ist aber noch keine konkrete Lösung. Die eigentliche Herausforderung besteht darin, das IT-Sicherheitsmanagement in bereits etablierte IT-Betriebsprozesse einzugliedern.

Die Referenten

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von Lokalen Netzen. Im Team der ComConsult Be-



ratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

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.-Ing. Hans Peter Mohn ist seit mehreren Jahren als IT-Berater tätig. Schwerpunkte seines Aufgabenbereichs bei der ComConsult Beratung und Planung GmbH sind die Durchführung von Sicherheitsüberprüfungen, die Erstellung und Umsetzung von Sicherheitskonzepten sowie die Organisation des Betriebs von IT-Sicherheitsmaßnahmen. Herr Mohn ist lizenzierter IT-Grundschutz-Auditor der BSI (Bundesamt für Sicherheit in der Informationstechnik).

In diesem Seminar lernen Sie

- welche Standards im Bereich der IT-Sicherheit eine Rolle spielen, speziell welche Konzepte hinter dem Grundschutzhandbuch des BSI und hinter BS7799 stehen
- wie Risikoanalyse und strukturiertes Sicherheitskonzept zusammenhängen und welche Elemente dabei zu berücksichtigen sind worauf es bei einer Zertifizierung ankommt
- wie Audits geeignet vorbereitet werden und für wen und welchen Anwendungsbereich sich eine Zertifizierung eignet
- am Beispiel der ITIL-Prozesse dargestellt, wie IT-Sicherheit in den IT-Betrieb integriert werden kann
- welche Prozesse bei der Umsetzung eines Sicherheitskonzepts beteiligt sind, wie sich diese Prozessstruktur in die IT-Landschaft eingliedert und welche Schlüsselelemente diese Prozesse lebendig erhalten
- welche Kostentreiber an der IT-Sicherheit beteiligt sind und wie mit dem scheinbaren Widerspruch von Wirtschaftlichkeit und Sicherheit umge-gangen werden kann

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sicherheit

Ich buche das Seminar
IT-Sicherheitsmanagement in der Praxis
vom 28.06. - 30.06.04 in Köln

(Preis € 1.690,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Studie des Monats IT-Infrastrukturen: Ergebnisse einer Umfrage

Gegenstand der Studie

Im zweiten Halbjahr 2003 führte ComConsult Beratung und Planung GmbH, eine Umfrage zum Thema IT-Infrastruktur unter einer Reihe von Unternehmen und öffentlichen Verwaltungen durch. Ziel der Umfrage, welche die Basis der vorliegenden Studie bildete, war festzustellen, welche Vorhaben im Rahmen des Aufbaus der internen IT-Infrastruktur weitgehend als abgeschlossen gelten und mit welchen Vorhaben sich die Unternehmen und Behörden weiterhin befassen bzw. befassen werden.
Die Fragen der Studie wurden zur Erleichterung der Beantwortung als Multiple-Choice-Fragen formuliert. In der Regel wurden die vier möglichen Antworten so geordnet, dass die erste Antwort einem weitgehend abgeschlossenen und die letzte Antwort einem weitgehend offenen Stand des Vorhabens entsprach.

Insgesamt wurden 60 Fragen gestellt, gegliedert in folgende Kapitel:

- Passive Netztechnik
- Aktive Netzkomponenten und Netzprotokolle
- Service Level Management und Netzbetrieb
- Netzsicherheit
- Zusätzliche netzbasierende Dienste (DHCP, DNS, Verzeichnisse, Server-Cluster, Storage, E-Mail, Sprachkommunikation, Unified Messaging, VPN, sicheres HTTP)
- Betriebssysteme

Lesen Sie im Folgenden im Detail die Fragen, die den Unternehmen gestellt wurden, die Antworten finden Sie im Report:

Passive Netz-Technik

- Welche Art von Tertiär-Verkabelung überwiegt?
- Liegen Messprotokolle für die Verkabelung vor?
- Muss bei Umzügen erfahrungsgemäß nachverkabelt werden?
- Wird WLAN-Technik eingesetzt?
- Wann wurde das Potential- und Erdungsverhalten der Verkabelung überprüft?
- Ist die Verkabelung zwischen den Verteilern mit Wegeredundanz, ringförmig oder sternförmig aufgebaut?
- Wie viel Fasern im Backbone zwischen den Gebäuden sind insgesamt belegt?
- Wie hoch ist der Anteil der Singlemode-Fasern an der Backbone-Verkabelung?
- Sind die Netz-Komponenten in Schränken untergebracht?
- Wie ist die Zugangsmöglichkeit zur Verteilertechnik?

Aktive Komponenten/ Protokolle

- Wie viele verschiedene LAN-Typen werden außer Ethernet/ Fast-Ethernet/Gigabit-Ethernet eingesetzt?
- Welcher Anteil der LAN-Anschlüsse arbeitet noch mit Shared LANs (Hubs)?
- Wie viele Endgeräte arbeiten in der größten Layer-2-Broadcast-Domäne?
- Wie viele Hersteller sind im Bereich aktiver Komponenten für den LAN-Bereich im Einsatz?
- Wie lange sind die installierten aktiven Komponenten bereits im Einsatz?
- Wie lange wird von Herstellerseite für die eingesetzten Modelle an aktiven Komponenten noch Support und Ersatzteillieferung geleistet?
- Wie hat sich der Ersatzteilpreis für Ihre Netz-Komponenten in den letzten 12 Monaten entwickelt?
- In welcher Größenordnung liegen die Umschaltzeiten von Redundanzen in Ihrem Netzwerk?
- Wie groß sind die Reserven im Bereich Ports für den Anschluss von Endgeräten?
- Wie viele Protokollfamilien (SNA, IPX/ SPX, DEC-Protokolle usw.) außer TCP/ IP werden im Netz übertragen?

Service Level-Fähigkeit / Netz-Betrieb

- Welcher Anteil der Zuständigkeiten für LAN, MAN, WAN, SAN, Voice und Verkabelung sind in einer Organisationseinheit zusammengefasst?
- Erfährt der Netz-Betrieb von Problemen eher durch eine zentrale Hotline, bei der die Anwender anrufen, oder durch direkte Anwenderanrufe?
- Welcher Anteil des Vernetzungsstandards (Komponententypen, Verschaltungslogik, Konfigurations-Festlegungen für Protokolle und Mechanismen, usw.) des Unternehmens ist schriftlich dokumentiert?
- Wird Netz-Management gezielt für Permanentüberwachung und Alarmie-rung benutzt?
- Ist für die Management-Funktionen Configuration Management, Problem Management, Change Management, Kapazitätsmanagement, Verfügbarkeitsmanagement, Eventualfall-Planung im Netz eine eindeutige Zuständigkeit festgelegt?
- Gibt es schriftlich festgehaltene Handzettel, festgelegte einheitliche Abläufe für typische Arbeiten im Netz-Bereich (Einbau einer neuen Komponente, Durchführung eines Umzugs, Anschluss eines neuen Endgeräts, usw.) und wird auch nach diesen gearbeitet?
- Welche Verfügbarkeit wird für das Netz gewährleistet?
- Können Fragen der folgenden Art für Ihr Netz sofort beantwortet werden: mittlere Auslastung/Fehlerraten auf den Uplinks, Server-Anschlüssen, Verlauf der Netzlast über den Tag hinweg, Entwicklung in den letzten Monaten?
- Inwieweit liegen Kabelspinne, ein logischer Plan des Netzes, Konfigurati-onsdokumentation zu aktiven Kompo-nenten, Rangierinformationen und Informationen über die Belegung von Netz-Dosen vor und werden für Planung und Fehlersuche benutzt?
- Werden Netz-Management, Komponenten-Management-Software und ein Statistik- und Protokoll-Analysator für die Fehlersuche eingesetzt?

Netz-Sicherheit

- Zu welchem Anteil ist eine explizit ausgearbeitete Sicherheitsrichtlinie für das Netz umgesetzt worden?
- Werden die folgenden Maßnahmen zum Schutz des Netzes und der darin angeschlossenen Geräte verwendet: Firewall, Paketfilter auf den Netz-Komponenten am Netzwerk-Ausgang, Intrusion Detection, starke Authentifizierung, Verschlüsselung bei E-Mail-Verkehr mit Externen?
- Gibt es einen IT-Sicherheitsprozess, in den der Netz-Bereich gezielt eingebunden wird?

IT-Infrastrukturen: Ergebnisse einer Umfrage

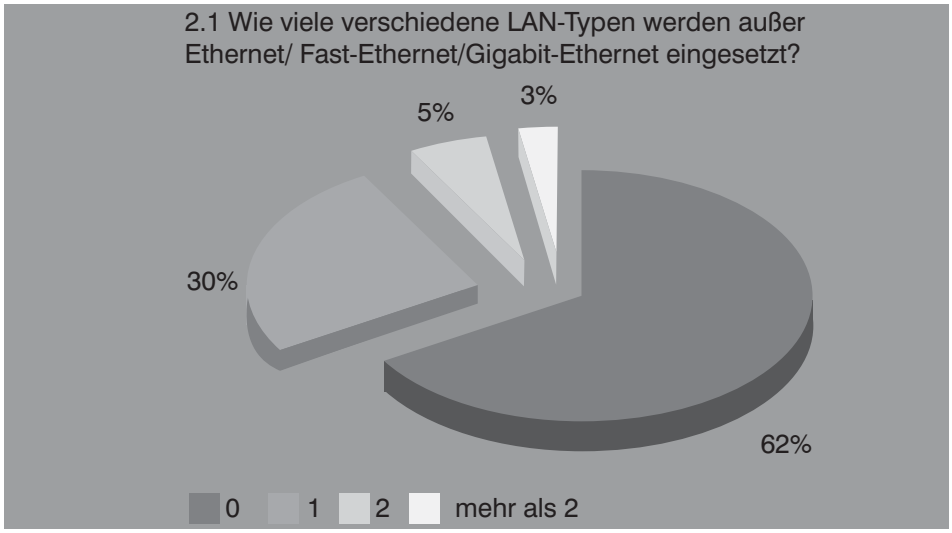
- Gibt es ein Notfallkonzept für größere Netz-Ausfälle, und werden die verschiedenen Notfälle eingeübt?
- Werden Sicherheitsüberprüfungen unter Einbeziehung des Netz-Bereichs durchgeführt?
- Wird das Netz-Personal ausdrücklich hinsichtlich Sicherheitsfragen geschult?
- Werden SNMP-communities und Telnet-Passwörter auf den Netz-Komponenten entsprechend allgemeinen Regeln für Passwörter gewählt, mindestens die Telnet-Passwörter regelmäßig geändert?
- Werden sicherheitsrelevante Aspekte im Zusammenhang mit Netz-Komponenten in die Netz-Überwachung (SNMP-Management) eingebunden und protokolliert?
- Werden Remote Administrations-Zugriffe gezielt und umfassend abgesichert, insbesondere mit starker Authentifizierung, VPN-Technik, gestuften Nutzer-Konten und unter gezielter Beschränkung der Möglichkeiten zur weiterführenden Kommunikation von administrierten Komponenten aus?
- Existieren für Sicherheitsvorfälle im Netz-Umfeld (Komponenten, Technikräume, usw.) Verhaltensregeln, klare Meldewege, Eskalationsstrategien und festgelegte Prioritäten?

Zusätzliche Services

- Zu welchem Anteil wird die IP-Konfiguration der Endgeräte mit DHCP gesteuert?
- Zu welchem Anteil arbeiten die Anwendungen mit DNS?
- Inwieweit ist eine unternehmensweite Verzeichnisstruktur realisiert?
- Inwieweit sind für wichtige Anwendungen Server-Cluster implementiert?
- Inwieweit ist ein Storage Area Network realisiert?
- Inwieweit ist ein einheitliches E-Mail-Konzept realisiert?
- Inwieweit ist ein einheitliches Sprachkommunikationskonzept realisiert?
- Inwieweit ist Unified Messaging realisiert?
- Inwieweit ist ein einheitliches IPsec-VPN realisiert?
- Inwieweit sind für wichtige Anwendungen Lösungen implementiert, mit denen die Benutzer über verschlüsselte Web Sessions auf die Anwendung zugreifen können?

Betriebssysteme

- Wie viele verschiedene Microsoft-Betriebssysteme werden im Serverbereich eingesetzt?
- Welcher Anteil der Microsoft-Server ist in ein einheitliches Domänen- bzw. Verzeichniskonzept eingebunden?
- Welche Betriebssysteme überwiegen im Microsoft-Server-Bereich?
- Wie viele verschiedene Microsoft-Betriebssysteme werden im Client-bereich eingesetzt?
- Welcher Anteil der Microsoft-Clients ist in ein einheitliches Domänen- bzw. Verzeichniskonzept eingebunden?
- Welche Betriebssysteme überwiegen im Microsoft-Client-Bereich?
- Bei welchem Anteil der Clients werden die Systemeinstellungen zentral vorgenommen und verteilt?
- Bei welchem Anteil der Clients erfolgt die Installation anhand eines Standard-Builds?
- Wie viele verschiedene Unix-Betriebssysteme (ohne Linux) werden eingesetzt?
- Wie viele verschiedene Linux-Varianten werden eingesetzt?



Fax-Antwort an ComConsult 02408/955-399

Bestellung IT-Infrastruktur

☐ Ich bestelle den Report

IT-Infrastruktur:
Ergebnisse einer Umfrage

(Preis € 198.-- zzgl. MwSt. und Versand)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Schwerpunktthema

Angriff auf DECT: Voice over WLAN

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.

1. Kanalzugriff in WLAN nach IEEE 802.11

Für den Kanalzugriff (Medium Access Control, MAC) sind in IEEE 802.11 zwei Verfahren spezifiziert worden:

- Die Distributed Coordination Function (DCF) ist ein verteilter zufallsgesteuerter Zugriffsmechanismus (Carrier Sense Multiple Access with Collision Avoidance, kurz: CSMA/CA), der einen Best-Effort-Dienst liefert.
- Die Point Coordination Function (PCF) ist ein zentral gesteuerter Mechanimus, bei dem die beteiligten Stationen in re-gelmäßigen Abständen durch einen Master (typischerweise ein Access Point) per Polling ein Senderecht erhalten. Auf diese Weise kann für die beteiligten Stationen eine gewisse Bandbreite zugesichert werden.

Die Implementierung der DCF ist in IEEE 802.11 zwingend vorgeschrieben, die Realisierung der PCF ist jedoch nur als optional klassifiziert. Daher wundert es nicht, dass in allen bekannten aktuellen Implementierungen lediglich die DCF umgesetzt wurde.

Das Grundprinzip der DCF ist dabei denkbar einfach: „Wer zuerst kommt mahlt zuerst!“. Die Funktionsweise der DCF wird im Folgenden anhand eines Beispiels beschrieben. Für eine detaillierte Beschreibung des Kanalzugriffs, speziell der DCF, siehe [1] und [2].

In dem hier betrachteten Beispiel sind drei Stationen A, B und C am Kanalzugriff beteiligt, wie in Abbildung 1 gezeigt. Es ist dabei vollständig unwesentlich, welche Station ein Access Point ist und welche Station ein Client-Adapter. Die DCF behandelt alle Teilnehmer gleichberechtigt. Station A überträgt gerade, Stationen B und C sind sendewillig. Eine sendewillige Station ermittelt zunächst mit einem Pseudozufallszahlengenerator aus einem speziellen Intervall eine Wartezeit (Backoff Time) und hört den Funkkanal ab. Im betrachteten Beispiel sind dies die Stationen B und C. Es sei angenommen, dass Station B eine kürzere Wartezeit „gewürfelt“ hat als Station C.

Beide Stationen stellen zunächst fest, dass eine andere Station (nämlich A) sendet. Am Ende der Sendung warten B und C eine festgelegte Zeitspanne ab, das so genannte DCF Inter Frame Spacing (DIFS).

Danach beginnt das Contention Window (CW), in dem sendewillige Stationen um den Kanal konkurrieren: Die beteiligten Stationen (hier B und C) starten einen Timer, der mit der entsprechenden Backoff Time initialisiert wurde und hören weiter den Funkkanal ab. Der Timer von Station B ist im Beispiel als erstes abgelaufen, und da der Kanal immer noch frei ist, beginnt Station B mit der Übertragung.

Station C erkennt die Übertragung und hält seinen Backoff Timer an und wartet auf das Ende der Übertragung.

Der Empfänger der Übertragung (im Bei-

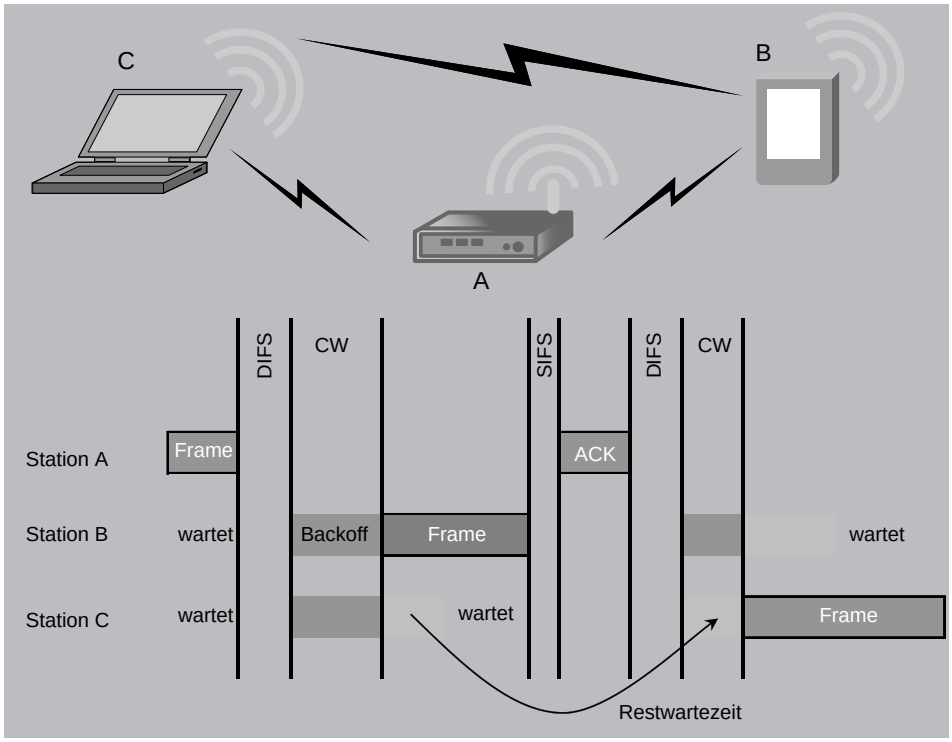


Abbildung 1: Beispiel für die Funktionsweise der Distributed Coordination Function (DCF)

spiel Station A) wartet am Ende der empfangenen Nachricht eine weitere festgelegte Zeitspanne ab, das so genannte Short Inter Frame Spacing (SIFS), und sendet unmittelbar danach ein Acknowledgement Frame (ACK). Das SIFS ist kürzer als das DIFS. Dies erlaubt, dass ein ACK unmittelbar nach einer empfangenen Sendung ohne Wettbewerb mit anderen Stationen gesendet werden kann. Natürlich werden nur Unicast-Pakete auf diese Weise quittiert. In einem gewissen Sinne wird die Übertragung eines ACK auf diese Weise bevorzugt, d.h. höher als alle „normalen“ Pakete priorisiert.

Nach Abwarten des DIFS läuft das CW und der zugehörige Backoff Timer für Station C weiter. Im Beispiel ist angenommen, dass C jetzt die kürzeste Restwartezeit hat. Nach Ablauf des Backoff Timers ist im Beispiel der Kanal also noch frei, und C beginnt mit der Übertragung.

Dieses Verfahren vermeidet nicht, dass zwei sendewillige Stationen zur gleichen Zeit den freien Kanal abhören und zur gleichen Zeit mit einer Sendung beginnen. In diesem Fall kommt es zu einer Kollision, die in Funknetzen nicht wie in einem kabelbasierten Netz unmittelbar erkannt werden kann. Eine Kollisionserkennung und -vermeidung kann in Funknetzen nur durch einen Rückkanal erfolgen. Auf Empfängerseite wird das Paket daher, wie im Beispiel gezeigt, quittiert. Bleibt diese Quittung aus, geht der Sender von einer Kollision (oder einem sonstigen Fehler bei der Funkübertragung) aus und startet, sofern die maximale Anzahl von Übertragungsversuchen nicht überschritten wird, eine erneute Übertragung des Pakets. Andernfalls wird das Paket verworfen.

Die Größe des Zeitintervalls, aus dem die Zufallszahl für die Backoff Time gewürfelt wird, wächst mit der Anzahl der Zugriffsversuche exponentiell bis zu einer maximalen Größe (Exponential Backoff). Analog zu CSMA/CD, dem Ethernet-Zugriffsverfahren, wird eine Station dadurch im Folgezugriffsversuch benachteiligt.

Die Erkennung durch Carrier Sensing, ob der Kanal frei oder belegt ist, funktioniert in Funknetzen jedoch nicht immer.

Nehmen wir beispielsweise zwei Clients, die in einer solchen Distanz zueinander stehen (oder durch ein Hindernis abgeschattet werden), dass sie sich gegenseitig nicht mehr empfangen können. Nehmen wir jetzt noch an, dass in der Mitte der beiden Stationen ein Access Point steht, so dass beide Clients den Access Point empfangen können. Überträgt nun ein Client an den Access Point und führt der zweite Client ein Carrier Sensing durch, geht der zweite Client von einem vermeintlich freien Kanal aus und beginnt seinerseits mit der Übertragung. Am Access Point kommt es dann zu einer Kollision. Dieses Beispiel beschreibt das für Funknetze typische so genannte Hidden-Station-Problem. Der Standard IEE 802.11 sieht hierzu ein als RTS/CTS (Request to Send/Clear to Send) bezeichnetes Verfahren vor, das an den Stationen im WLAN bei Bedarf aktiviert werden kann (siehe hierzu [1]).

2. Ohne Quality of Service geht es nicht

Eigentlich sind WLAN nach IEEE 802.11, die nur die DCF implementiert haben, für Dienste, die eine gewisse Gütegarantie erfordern, alles andere als geeignet. Die Gleichberechtigung aller Teilnehmer ist ein Grundprinzip der DCF, und in einem Shared Medium ist dies eigentlich Gift für Quality of Service (QoS). Die DCF sieht weder eine Priorisierung unterschiedlicher Verkehrsklassen noch eine explizite Bandbreitenreservierung vor. Als Konsequenz ist die Antwortzeit in einem WLAN nach IEEE 802.11 stets starken Schwankungen unterworfen. Diese Schwankungen sind neben der Qualität des Funkkanals abhängig von der Anzahl der Clients, die an einem Access Point assoziiert sind und vom Verkehrsverhalten (also von den Anwendungen) dieser Clients.

Andererseits ist die Forderung nach der Unterstützung von QoS in WLAN naheliegend. Treibende Kraft ist hier natürlich die Sprachübertragung über ein WLAN. Hintergedanke ist der verständliche Wunsch, drahtlose Kommunikationsdienste über eine einzige Funkinfrastruktur abzuwickeln. Hier kommen grundsätzlich drei Ansätze in Frage:

- Erweiterung eines schnurlosen Telekommunikationssystems (also typischerweise DECT) um eine Komponente zur „schnellen“ Übertragung von Daten
- Integration von DECT und WLAN in ein gemeinsames System
- Erweiterung von WLAN um QoS-Konzepte

Der erste Ansatz ist seit vergleichbar langer Zeit verfügbar, da DECT von Anfang an auch Datendienste mit den ISDN-typischen Datenraten (und Übertragungskonzepten) vorgesehen hat, konnte sich jedoch nie gegen WLAN durchsetzen. HomeRF, ein WLAN-Standard für den privaten und den SOHO-Einsatz, hat eine Integration der Frequency-Hopping-Variante von DECT bei 2,4 GHz vorgesehen, d.h. den zweiten Ansatz verfolgt (siehe [5]). Technisch ist HomeRF zwar ein höchstinteressantes System, das verantwortliche HomeRF-Gremium hat seine Arbeit jedoch Anfang 2003 eingestellt.

Es bleibt also die dritte Alternative. Seit geraumer Zeit sind zwar VoIP over WLAN Handsets verfügbar (als Beispiele seien nur die Geräte von Symbol und SpectraLink genannt), die jedoch proprietäre Verfahren einsetzen, um zumindest eine Priorisierung des VoIP-Verkehrs zu ermöglichen. Client Adapter und Access Point müssen also hier besonders aufeinander abgestimmt sein. Ein Access Point des Herstellers Symbol erkennt beispielsweise Pakete eines Symbol VoIP Handsets anhand des herstellerspezifischen Teils der MAC-Adresse und ist so in der Lage, diese Pakete vorrangig zu anderen zu behandeln, um die Antwortzeit für diese Clients zu reduzieren. Richtig in Bewegung ist der Markt allerdings erst gekommen, als sich erste Ergebnisse der Standardisierungsbemühungen der Arbeitsgruppe „e“ von IEEE 802.11 abzeichneten. Im Folgenden werden wir den Stand der Dinge analysieren und das Produkt eines der Handset-Anbieter genauer unter die Lupe nehmen.

Neben VoIP over WLAN gibt es natürlich auch eine steigende Zahl von WLAN-Anwendungen in Produktions- und Logistikbereichen, die mit Anforderungen an das Antwortzeitverhalten gekoppelt sind und so von QoS-Konzepten in WLAN ebenfalls unmittelbar profitieren würden.

3. Quality of Service in IEEE 802.11e: Der Trick mit den Wartezeiten

Seit Mai 2000 arbeitet die „Task Group e“ der IEEE 802.11 an einer Erweiterung des MAC Layers, um in einem gewissen Rahmen eine Dienstgüte (QoS) sicherzustellen. Diese Arbeit wird in die Erweiterung IEEE 802.11e münden. Der Standard liegt aktuell lediglich als interner Draft vor. Obwohl noch nicht alle Details entschieden sind, zeichnet sich inzwischen die grundsätzliche Richtung für IEEE 802.11e ab (siehe [3]).

Wesentlich ist zunächst die Forderung der Abwärtskompatibilität zur bisherigen DCF. Damit verbietet sich die Möglichkeit der Implementierung von hochwertigen Kanalzugriffsverfahren, wie beispielsweise in HIPERLAN/2 spezifiziert (siehe [6]).
Neben der abwärtskompatiblen Erweiterung der bisherigen DCF um Priorisierungsmechanismen (Enhanced DCF,

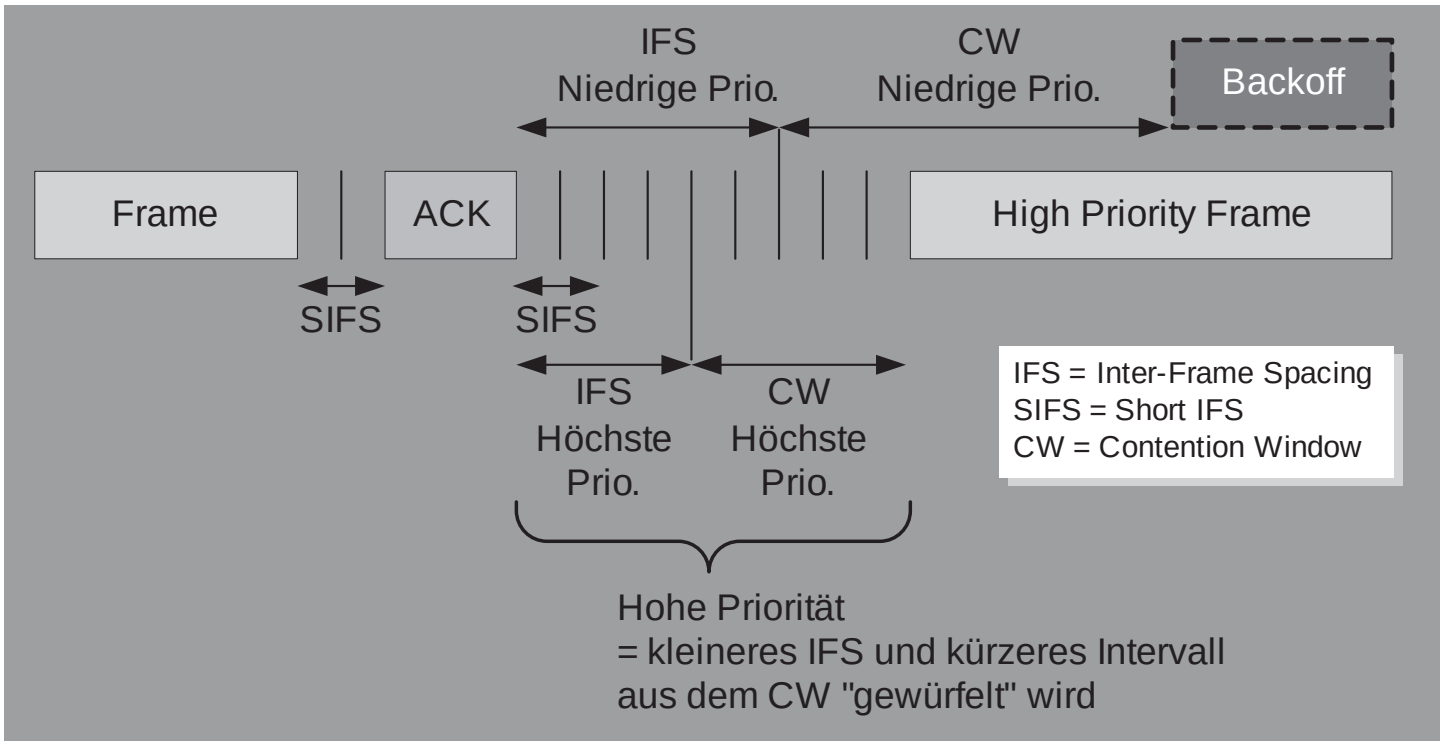


Abbildung 2: Priorisierung durch Wartezeiten mit der EDCF

EDCF) wird ein Burst-Modus, eine spezielle Polling-Funktion (Hybrid Coordination Function, HCF) und die Möglichkeit des Einsatzes von Forward Error Correction (FEC) im MAC Layer spezifiziert. In aktuell verfügbaren Systemen ist meist lediglich die EDCF des IEEE 802.11e Draft-Standards implementiert. Daher werden wir schwerpunktmäßig im Folgenden auf die EDCF eingehen.

Die EDCF wird an folgenden Bereichen Erweiterungen der DCF vornehmen:

- Anstelle einer einzigen Verkehrsklasse werden acht unterschiedlich priorisierteVerkehrsklassen unterschieden. In einer Station werden Pakete einer höheren Priorität beim Kanalzugriff bevorzugt behandelt.

- Anstelle des bisherigen DCF Inter-Frame Spacing (kurz DIFS) wird für je eine Verkehrsklasse i ein eigenes Inter-Frame Spacing festgelegt, das sogenannte Arbitration Inter-Frame Spacing, kurz AIFS[*i*]. Stehen zu einem Zeitpunkt von zwei Stationen Pakete zur unmittelbaren Übertragung an, hat das Paket mit dem kürzeren AIFS automatisch Vorrang vor dem Paket der anderen Station mit dem längeren AIFS, wie in Abbildung 2 illustriert. Genau dieses Prinzip wird bereits in der DCF zur Priorisierung eines ACK genutzt.

- Damit im Vergleich zu den anderen Verkehrsklassen ein Paket einer höher priorisierten Verkehrsklasse im Mittel einen schnellen Kanalzugriff erhält, werden für jede Verkehrsklasse i eigene Parameter CWmin[i] und CWmax[i] für die Berechnung der Größe des Contention Window (CW) festgelegt. Diese Berechnung geschieht nach folgendem Verfahren: Eine Station, die ein Paket der Verkehrsklasse i senden möchte, berechnet die Wartezeit CW aus dem Produkt einer Pseudozufallszahl p und aus der systemspezifischen Dauer eines Slots S, d.h. $CW = p \times S$. Für IEEE 802.11 und IEEE 802.11b beträgt der Wert von S (im Standard als aSlotTime bezeichnet) 20 μs und für ein OFDM-System gemäß IEEE 802.11a bzw. 802.11g sind es 9 μs. Die Pseudozufallszahl p ist eine ganze Zahl, die gemäß einer Gleichverteilung aus der Menge {0, ... CW1[i]} „gezogen“ wird. Dabei ist CW1[i] = CWmin[i] gesetzt. Je kleiner der Wert von CWmin[i] desto geringer die maximale und die mittlere Wartezeit. Eine Verkehrsklasse höherer Priorität erhält also einfach einen kleinen Wert für CWmin, um im Mittel bevorzugt behandelt zu werden. Der Standard gibt hierzu Default-Werte vor, die jedoch grundsätzlich vom Nutzer angepasst werden können. Sollte das Paket seinen Empfänger nicht erreichen (durch eine Kollision oder einfach bedingt durch den störanfälligen Funkkanal) oder das zu dem Paket gehörige ACK „verloren“ gehen, wird eine Neuübertragung des Pakets versucht. Das Intervall {0, ... CWn[i]}, aus dem für den nächsten (n-ten) Sendeversuch wieder eine Zufallszahl gezogen wird, wächst exponentiell (zur Basis 2) mit der Anzahl der Übertragungsversuche n gemäß

$$CW_n(i) = 2CW_{n-1}(i) + 1,$$
$$CW_1(i) = CW_{min}(i)$$

Damit wird auch im Falle der Wiederholung eines Übertragungsversuchs im Mittel die Wartezeit eines Pakets hoher Priorität geringer sein als die entsprechende Zeit eines Pakets geringerer Priorität. Das Intervall für eine niedrige Priorität wächst sogar „dramatisch“ schneller. Andererseits wird auch für eine hochpriore Verkehrsklasse die Wartezeit länger, so dass bei Wiederholungen einer Übertragung die Erstübertragung einer niedriger priorisierten Übertragung nicht automatisch das Nachsehen hat (ein Gebot der Fairness des Verfahrens).
Insgesamt ergeben sich bei dem vorgestellten Verfahren für eine Verkehrsklas-se hoher Priorität im Mittel kleinere Werte für CW und damit kürzere Wartezeiten bis zum Zugriff auf das Medium. Als Konsequenz verringert sich insge-

samt auch die Varianz der Antwortzeit, was ein entscheidender Faktor bei der Sprachüber- tragung ist.

Für die EDCF ist in IEEE 802.11e keine Admission Control vorgesehen. Simulationen und Prototypstudien haben ergeben, dass der Mechanismus der EDCF und der HCF hinsichtlich der Fairness als kritisch einzustufen ist. Bei einer genügend großen Zahl von Stationen mit hoher Priorität und einem entsprechenden Verkehrsaufkommen leidet der Verkehr niedrigerer Priorität massiv (siehe z.B. [7]).

4. Zellwechsel in WLAN: Nahtlos muss er sein!

Besonders kritisch für die Sprachübertragung über WLAN ist das Verhalten beim Wechsel zwischen Funkzellen während der Kommunikation, d.h. während des Gesprächs. Der Wechsel sollte nach Möglichkeit nicht wahrnehmbar sein bzw. zumindest nicht zu einer deutlichen (als unangenehm wahrgenommenen) Verschlechterung der Verbindung führen. In der Mobilfunkgemeinde wird der Wechsel eines Kanals unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung als Handover bezeichnet.

Bedenkenswert ist nun, dass der Standard IEEE 802.11, bis auf die Feststellung, dass ein Handover (in IEEE 802.11 als BSS Transition bezeichnet, in der WLAN-Gemeinde auch oft missverständlich Roaming genannt) zu unterstützen sei, keinerlei Festlegungen bezüglich der Verfahren und Parameter für einen Handover macht.

Die Handover-Funktion ist also vollständig dem Hersteller überlassen.

Dies ist oft auch ein Problem für klassische WLAN-Anwendungen, die eine uneingeschränkte Mobilität ohne (zeitweiligen) Verlust der Ende-zu-Ende-Kommunikation auf einem größeren Gebiet erfordern. Wenn dieses Gebiet mit mehreren Funkzellen (unter Berücksichtigung von Ausbreitungseigenschaften und Verkehrsanforderungen) abgedeckt werden muss, ist die Handover-Funktion essentiell. Während TCP noch „Aussetzer“ von mehreren Sekunden beim Zellwechsel verkraftet, ist dies für UDP-basierte Anwendungen nicht selten ein Problem und speziell für eine Sprachübertragung nicht akzeptabel.

Ein Handover wird in WLAN nach IEEE 802.11 stets durch den Client initiiert (Abbildung 3). Der Standard IEEE 802.11 legt dabei keine spezielle Kommunikation zwischen Client und Access Point bzw. zwischen den Access Points fest. Der Zellwechsel geschieht einfach durch eine Assoziierung des Clients am neuen Access Point. Die Assoziierung am alten Access Point bleibt zunächst bestehen, bis sie nach Ablauf einer gewissen Zeitspanne für inaktive Clients schließlich aus der Assoziierungsliste gelöscht wird. Dies stellt ein Problem bei Inter-Client-Kommunikation über einen Access Point dar: Solange einem Access Point nicht bekannt ist, dass der Client die Funkzelle verlassen hat, leitet er die Pakete an die MAC-Adresse des Clients nicht über das Festnetz weiter. Dies bedeutet, dass die in der Funkzelle verbliebenen Stationen mit dem Client, der die Funkzelle verlassen hat, nicht kommunizieren können. Die Access Points mancher Hersteller kommunizieren an dieser Stelle miteinander, damit bei einem Handover ein Client sofort aus der Assoziierungsliste des alten Access Points gelöscht werden kann.

Die Entscheidung für ein Handover trifft der Client anhand einer Bewertung der Qualität der Funkverbindung. Wird die Verbindung zum aktuellen Access Point als zu schlecht eingestuft, muss der Client versuchen, einen Access Point mit besseren Empfangsbedingungen zu finden. Hierzu muss der Client ein Scanning der einzelnen WLAN-Kanäle (1 bis 13 bzw. 1 bis 11 für FCC-Adapter) durchführen. Dabei sucht der Client-Adapter nach einem Access Point mit besseren Empfangsbedingungen. Zusätzlich kann als Parameter die aktuelle Auslastung eines Access Points in die Auswahl eines geeigneten Access Points mit einfließen. Der Client kann durchaus gewisse Kanäle bevorzugt durchsuchen, um einen geeigneten Access Point mit möglichst geringem Aufwand zu finden.

Die Bewertung der Empfangsqualität auf einem Kanal kann durch verschiedene Methoden erfolgen. Der Standard IEEE 802.11 liefert lediglich grundlegende Hilfsmittel:

- Über einen Primitiv zum Physical Layer kann (als relativer Wert) die aktuelle Re-

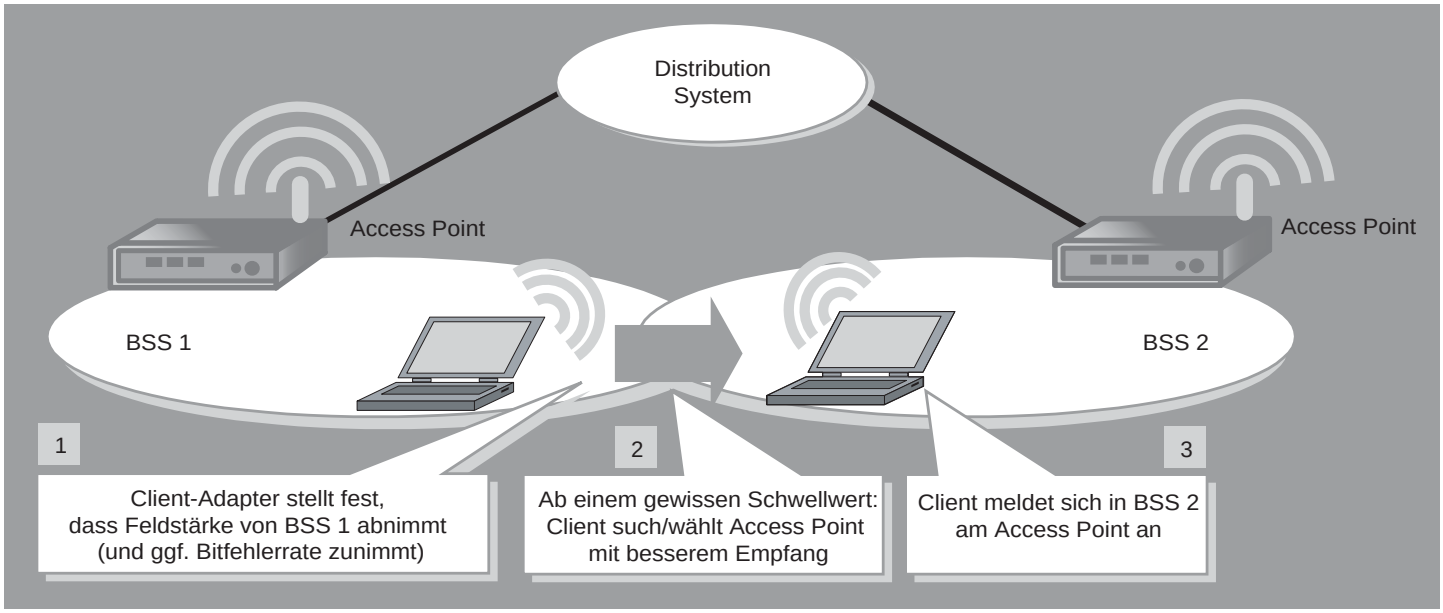


Abbildung 3: Grundsätzliche Funktionsweise eines Handovers

ceived Signal Strength Indication (RSSI) und die Signal Quality erfragt werden.
- Über Zähler in der IEEE 802.11 MIB kann aus der Anzahl der CRC-Fehler oder der Anzahl von Re-Transmissions ein Qualitätsindikator abgeleitet werden.

Selbst wenn ein perfektes Bewertungskriterium für die momentane Qualität eines Funkkanals möglich wäre, könnte es kein optimales Handover-Verfahren geben. Zunächst verhält sich ein Funkkanal immer (mehr oder weniger) zufällig. Die Feststellung, dass der Kanal aktuell eine gute Qualität aufweist, heißt noch lange nicht, dass im nächsten Moment diese Qualität bestehen bleibt.

Zusätzlich hängt ein Handover-Verfahren stark davon ab, mit welcher Empfindlichkeit eine Handover-Entscheidung getroffen wird. Ein System mit hoher Empfindlichkeit, das beispielsweise schon bei kleinen Verschlechterungen des RSSI reagiert und einen besseren Access Point sucht, wird zwar schnell ein Handover durchführen, dies vielleicht aber zu oft und teilweise auch überflüssigerweise. Da ein Handover immer mit einem gewissen Verlust behaftet ist, kann sich in einem System, das zu empfindlich eingestellt ist, im Extremfall ein Ping-Pong-Effekt einstellen. Dabei kann das System mit nichts anderem als einem Handover von einem Access Point zum anderen beschäftigt sein. Umgekehrt führt ein System, das nur mit einer niedrigen Empfindlichkeit reagiert, zu einem Trägheitseffekt, bei dem der Client trotz Qualitätseinbußen in der Kommunikation an dem aktuellen Access Point „klebt“, obwohl sich der Client vielleicht schon in der unmittelbaren Nähe eines anderen Access Points befindet. Gerade das letztere Verhalten ist für die Sprachübertragung sehr unangenehm, da es hier oft erst zu Paketverlusten kommt, bevor das Handover durchgeführt wird.

Die Übertragung von Sprache ist zwar keine bandbreitenintensive Anwendung, benötigt allerdings einen kontinuierlich verfügbaren Kanal, dessen Delay-Verhalten nicht allzu großen Schwankungen unterliegen darf. Daher ist es akzeptabel, dass ein WLAN-Handset während der Sprachübertragung gewisse Durchsatzeinbußen durch ein regelmäßiges Scanning der Funkkanäle nach verfügbaren Access Points hinnimmt, um im Falle eines Zellwechsels sofort zu wissen, wohin der Wechsel durchgeführt werden soll. Ein Handover sollte für die Sprachübertragung geschwindigkeitsoptimiert ablaufen. Eine durchsatzoptimierte Implementierung (wie sie oft für Client-Adapter für Notebooks realisiert ist) würde ein Scanning der Funkkanäle nur bei Bedarf durchführen, also erst bei einer Verschlechterung der Qualität des Funkkanals.

Da IEEE 802.11 an dieser Stelle keine Vorgaben macht, ist es herstellerspezifisch, ob und wie der Nutzer das Handover-Verhalten steuern kann.

Erst in der Erweiterung IEEE 802.11f, die im Juni 2003 verabschiedet wurde, ist ein-Inter Access Point Protocol (IAPP) standardisiert worden, welches es bei einem Zellwechsel erlaubt, die Client-spezifischen Informationen (speziell die Sicherheitseinstellungen) über das Distribution System vom bisherigen Access Point zum neuen Access Point zu übertragen. Das IAPP ist von Bedeutung, wenn Wi-Fi Protected Access (WPA) bzw. IEEE 802.11i genutzt wird, da hier eine Authentifizierung des Nutzers über IEEE 802.1x durchgeführt wird. In diesem Fall ist es geschickter, die Sitzungsinformationen über das Distribution System vom alten zum neuen Access Point zu transportieren, anstatt eine erneute Authentifizierung vorzunehmen.

Ein IAPP wird von manchen Access Points schon seit geraumer Zeit unterstützt, meist jedoch noch in einer proprietären Variante.

5. Leistung von VoIP over WLAN am Beispiel Cisco 7920

Access Points, die QoS-Konzepte aus der Arbeit der Task Group „e“ von IEEE 802.11 implementieren, gibt es inzwischen einige. Da der Standard IEEE 802.11e noch nicht verabschiedet ist und sich in der Vergangenheit die Konzepte von Version zu Version des Draft-Standards im Detail geändert haben, muss damit gerechnet werden, dass in den Produkten künftig noch Firmware-Aktualisierungen anstehen. Weiterhin sind VoIP-Handsets für IEEE 802.11b von verschiedenen Herstellern verfügbar. Im Gegensatz zu der Access-Point-Seite gibt es hier noch keine Implementierungen nach dem Draft-Standard zu IEEE 802.11e, und im Detail sind noch diverse herstellerspezifische Mechanismen verborgen. Im Hinblick auf eine baldige Verabschiedung von IEEE 802.11e ist es trotzdem sinnvoll, sich genauer mit der Leistung von VoIP over WLAN zu befassen.

Im Testlabor der ComConsult haben wir exemplarisch das Handset 7920 von Cisco (Abbildung 4) in einer Konfiguration mit dem Cisco CallManager 4.0 und den verschiedenen Cisco Aironet Access Points (350, 1100 und 1200) getestet. Das 7920 nutzt IEEE 802.11b zur Funkübertragung und „spricht“ das Skinny-Signalisierungsprotokoll zur Kommunikation mit dem Cisco CallManager. Die Cisco Access Points implementieren eine EDCF basierend auf dem Draft-Standard zu IEEE 802.11e. Schwerpunkt der Tests war die Untersuchung der folgenden Fragestellungen:

Abbildung 4:
Getestetes VoIP-Handset 7920 von Cisco

- Wie wirken sich die QoS-Mechanismen unter verschiedenen Auslastungen des WLAN tatsächlich aus, und kommt es wirklich zu spürbaren Effekten? Ist die (subjektive) Sprachqualität vergleichbar zu DECT?
- Ist ein Zellwechsel von einem Access Point zu einem anderen während des Gesprächs ohne Probleme möglich oder kommt es zu einer signifikanten Verschlechterung der Sprachqualität bis hin zu einem zeitweiligen Abbruch der Kommunikation?

Um es vorweg zu nehmen: Wir waren ausgesprochen angenehm überrascht!

Unsere ersten Versuche mit VoIP-Handsets für IEEE 802.11b, die wir vor fast drei Jahren durchführten, hatten zwar gezeigt, dass die Sprachübertragung prinzipiell funktioniert. Von einer Qualität und Mobilität, wie man sie seit Jahren von DECT gewohnt ist, war man zum damaligen Zeitpunkt allerdings noch weit entfernt. Dies ist der Grund, weshalb in unserem eigenen Gebäude trotz einer seit dem Jahr 2000 produktiv eingesetzten flächendeckenden VoIP-Lösung und trotz der Verfügbarkeit von WLAN noch einige DECT-Endgeräte genutzt werden.

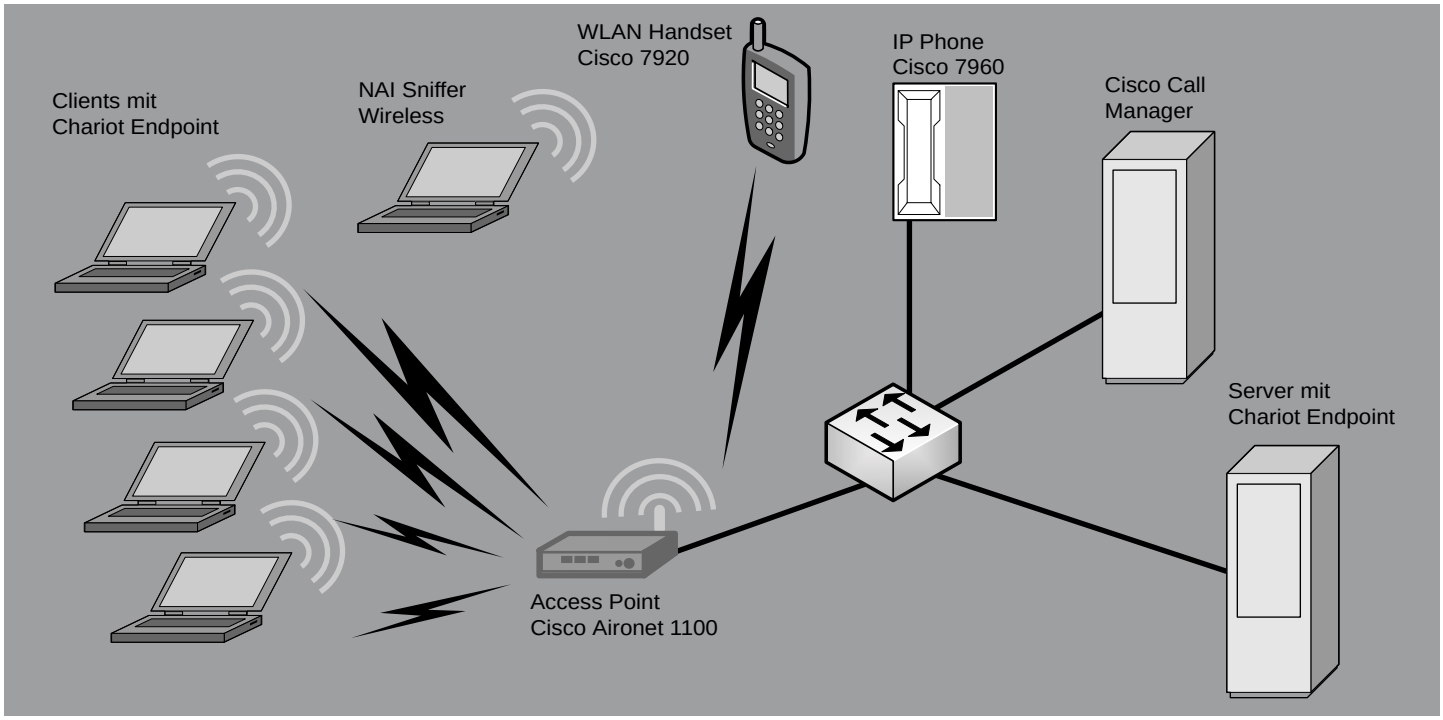


Abbildung 5: Testkonfiguration zur Überprüfung der Wirksamkeit der EDCF

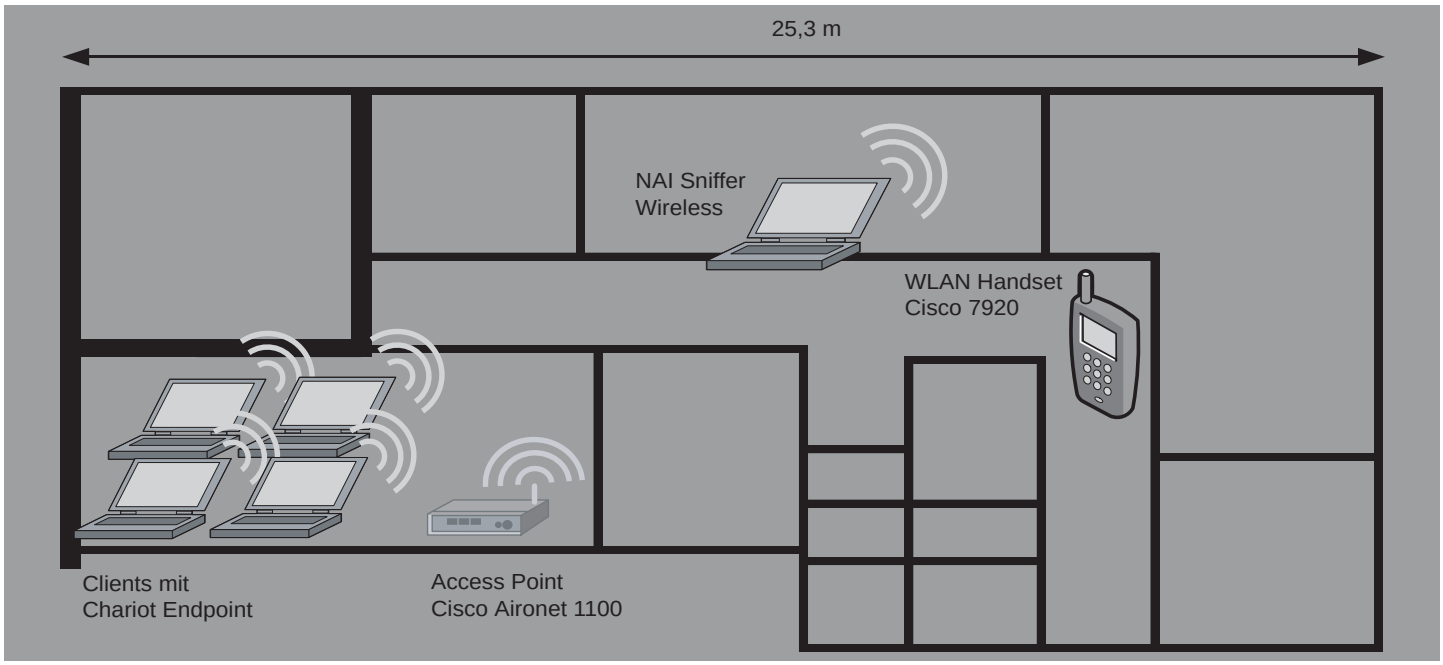


Abbildung 6: Räumliche Anordnung von Clients und Access Point

5.1 Wirksamkeit der QoS-Mechanismen

Die Testkonfiguration bestand, wie in Abbildung 5 gezeigt, aus folgenden Komponenten:

- Cisco Aironet 1100 Access Point (Firmware-Version 12.2(13)JA1)
- Cisco CallManager 4.0
- Cisco 7920 Handset (Firmware-Version 1.06)
- Cisco 7960 IP Phone
- Vier Notebooks mit NetIQ Chariot Endpoints zur Erzeugung von Last auf der Luftschnittstelle und ein PC im LAN mit NetIQ Chariot Endpoint als Server
- Ein Notebook mit NAI Sniffer zur Aufzeichnung und Analyse auf der Luftschnittstelle

Abbildung 6 illustriert hierzu die räumlich Anordnung und den Abstand zwischen WLAN-Stationen und Access Point.

Am Cisco Access Point werden die QoS Parameter im Rahmen einer QoS-Policy festgelegt. Die Identifikation bzw. Festle-

Angriff auf DECT: Voice over WLAN

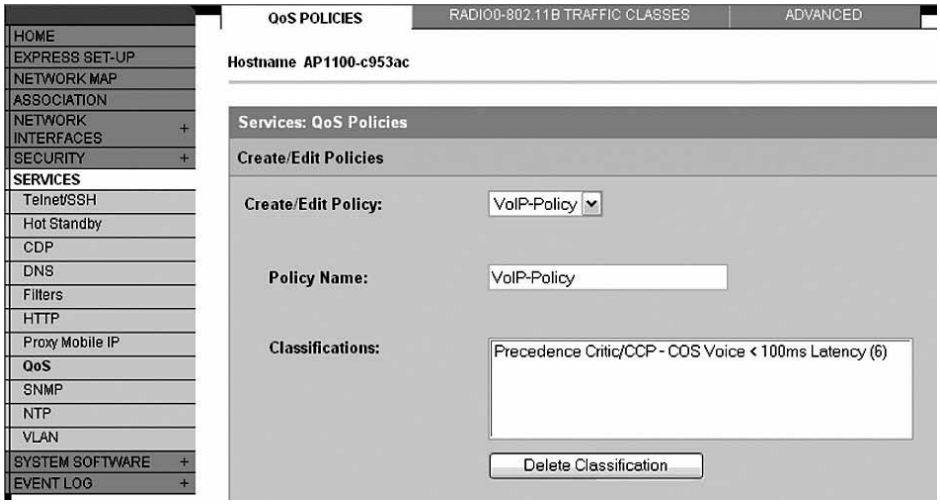


Abbildung 7: Definition einer QoS-Policy mit Angabe der Verkehrsklassifizierung

gung einer Priorisierung erfolgt nutzerdefiniert über eine Markierung gemäß IP ToS/ DiffServ und IEEE 802.1D/p (Abbildung 7). Hiermit wird für ein Paket, das der Access Point über die Luftschnittstelle übertragen soll, eine Zuordnung zu einer der Verkehrsklassen gemäß IEEE 802.11e vorgenommen. Die Default-Einstellungen (gemäß Draft IEEE 802.11e) zur Bestimmung des Contention Window für die einzelnen Verkehrsklassen können vom Benutzer angepasst werden (Abbildung 8).

Hostname AP1100-c953ac — AP1100-c953ac uptime is 1 day, 7 hours, 55 minutes

Services: QoS Policies - Traffic Class Definition

Class of Service	Min Contention Window (2^x-1; x can be 0-10)	Max Contention Window (2^x-1; x can be 0-10)	Fixed Slot Time (2-20)
Best Effort	5	10	2
Background	6	10	3
Spare	5	10	3
Excellent Effort	5	10	2
Controlled Load	4	10	2
Video <100ms Latency	4	8	2
Voice <100ms Latency	2	8	2
Network Control	3	8	2

Abbildung 8: Parameter zur Bestimmung der Größe des Contention Window

Nun ist es naheliegend, dass die QoS-Mechanismen erst bei einem entsprechend ausgelasteten System eine Wirkung zeigen, denn erst bei genügend hoher Konkurrenz um das Medium entsteht eine Notwendigkeit für eine Priorisierung. Damit ein entsprechender Hochlastfall im Test geeignet simuliert werden kann, wurde das Werkzeug Chariot von NetIQ eingesetzt. Dabei wurden kontinuierlich (d.h. ohne beabsichtigte Zeitverzögerung zwischen den Übertragungen) große Datenmengen per TCP zwischen vier Clients und einem Server in beide Richtungen über die Luftschnittstelle übertragen.

Folgendes Verhalten wird erwartet: Bei Einsatz von QoS in einer hoch belasteten Funkzelle sind für einen höher priorisierten Verkehrsstrom Mittelwert und Varianz der Zeitdifferenz zwischen MAC-Paketen deutlich niedriger als bei Verzicht auf QoS.

Abbildung 9 zeigt hierzu für die Kommunikationsrichtung vom Access Point zum 7920 Handset hin die Zeitdifferenz zwischen der Übertragung eines RTP-Pakets und einem davor (von einer der Stationen in der WLAN-Zelle, inklusive ACKs) gesendeten MAC-Paket bei Verzicht auf die Verwendung von QoS. Subjektiv wurde die Sprachqualität hier als schlecht bewertet. Abbildung 10 zeigt die Übertragung des selben Sprach-Samples bei aktivierter QoS-Funktion. Es zeigt sich deutlich, dass die Wartezeit für die RTP-Pakete erheblich reduziert ist. Subjektiv wurde die Sprachqualität hier als zufriedenstellend bewertet, trotz der extrem hohen Hintergrundlast.

Dies wird auch bestätigt, wenn direkt der zeitliche Abstand zwischen zwei RTP-Paketen betrachtet wird, wie in Abbildung 11 und Abbildung 12 gezeigt. Die EDCF führt

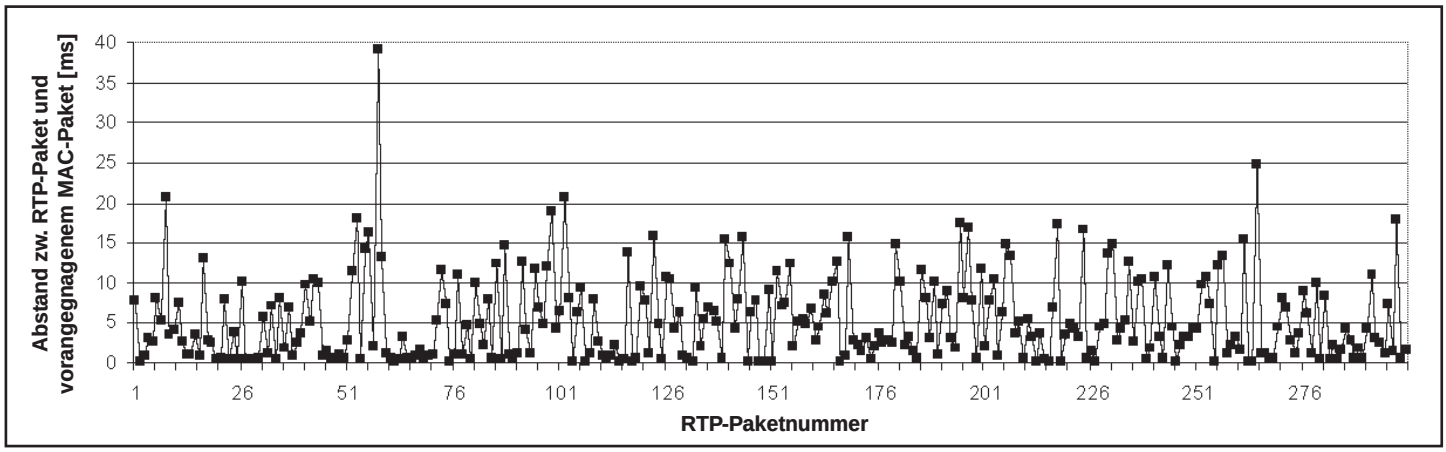


Abbildung 9: Abstand zum vorangegangenen MAC-Paket für Sprachpakete zum 7920 Handset ohne Priorisierung der Sprachpakete (subjektives Empfinden: sehr schlechte Qualität)

zu einer deutlichen Reduktion von Mittelwert und Varianz des Abstands zwischen den RTP-Paketen. Zwar hat eine VoIP-Station stets auch einen internen Puffer, der in einem gewissen Umfang die Delay-Schwankungen ausgleichen kann, dieser ist jedoch nicht allzu groß bemessen (da ansonsten die Verzögerung wieder zu groß wird).

Abschließend zeigt Abbildung 13 den Vergleich des Jitters, der den Effekt der EDCF noch unterstreicht. Wir haben diese Tests unter verschiedenen Lastszenarien und Abständen zwischen 7920 Handset und Access Point durchgeführt und können zusammenfassend feststellen, dass die EDCF eine wesentliche Funktion für die

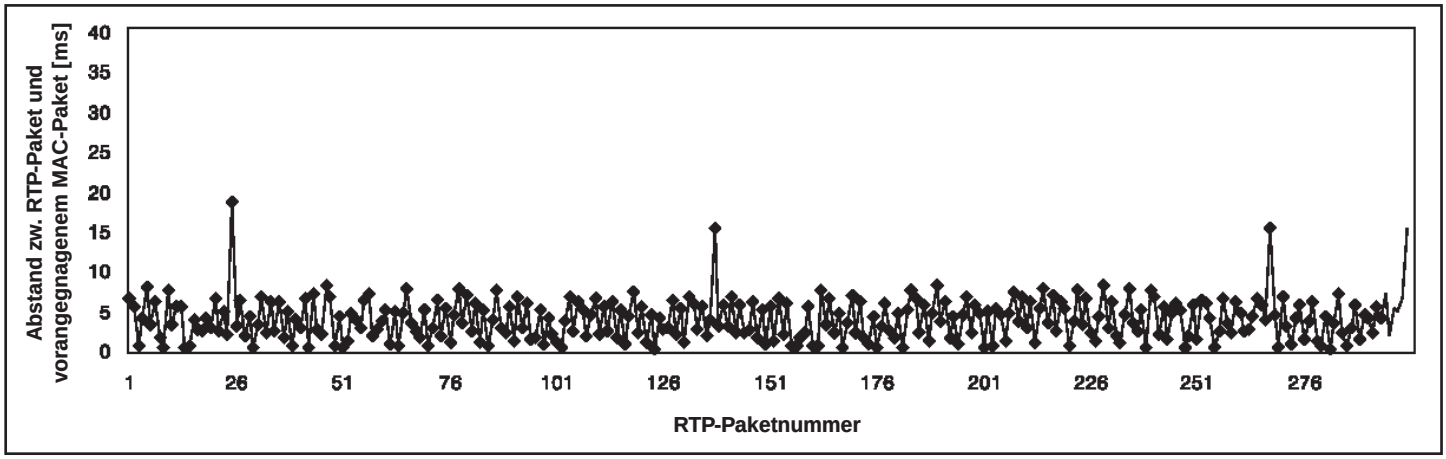


Abbildung 10: Abstand zum vorangegangenen MAC-Paket für Sprachpakete zum 7920 Handset unter Priorisierung von Sprachpaketen durch die EDCF (subjektives Empfinden: zufriedenstellende Qualität)

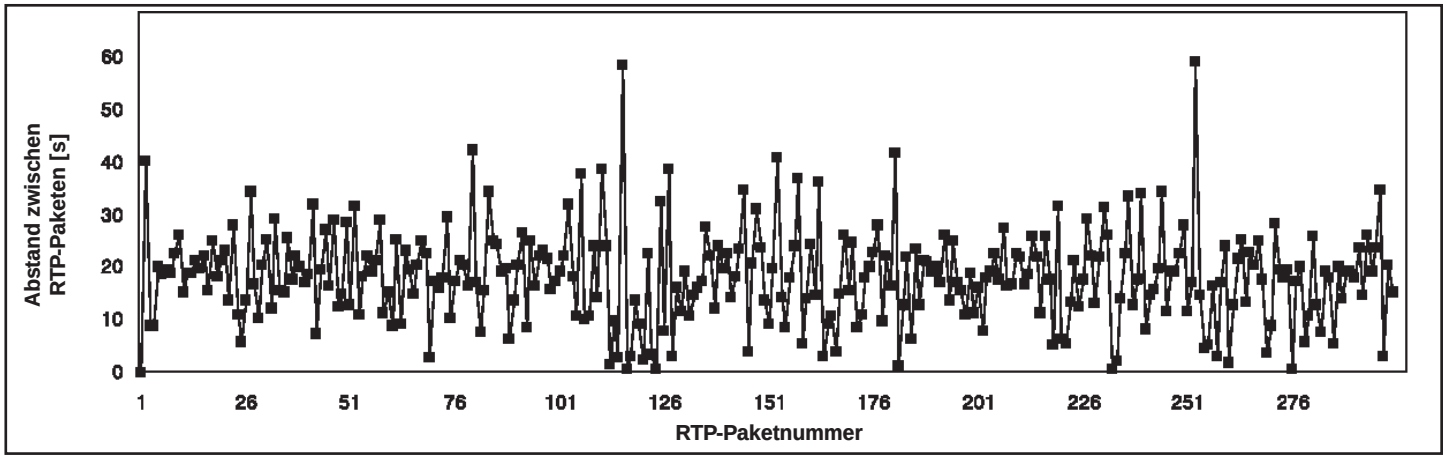


Abbildung 11: Abstand zum vorangegangenen RTP-Paket zum 7920 Handset ohne Priorisierung der Sprachpakete

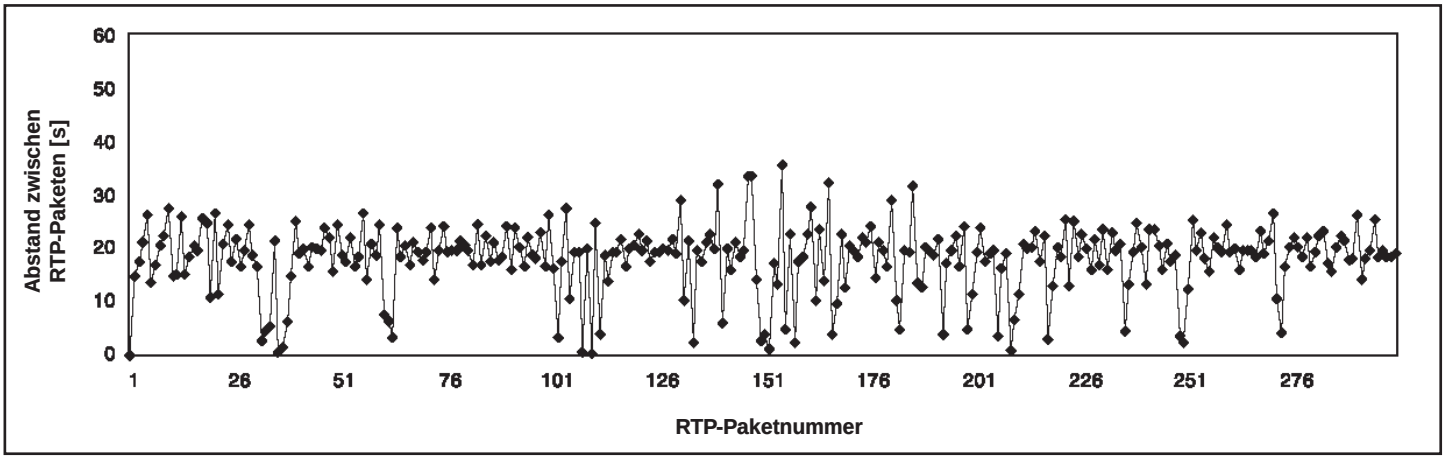


Abbildung 12: Abstand zum vorangegangenen RTP-Paket zum 7920 Handset unter Priorisierung von Sprachpaketen durch die EDCF

Koexistenz zwischen klassischer WLAN-Nutzung und der Übertragung von Sprache über ein WLAN darstellt.

Konkurrieren jedoch mehrere Handsets um den Funkkanal zur Übertragung von Sprachpaketen, so hilft die EDCF natürlich nicht. Untereinander sind die Stationen einer Verkehrsklasse gleichberechtigt, und da kein Admission Control stattfindet, käme es früher oder später zu höheren Schwankungen der Abstände zwischen den einzelnen Paketen, was letztendlich als schlechte Sprachqualität empfunden würde.
Die RTP-Analyse wurde mit Ethereal durchgeführt. Dieser Open Source Protocol Analyzer unterstützt nicht nur eine Vielzahl von Protokollen und erlaubt die Analyse eines RTP-Streams, sondern bietet auch die Möglichkeit des Abspeicherns eines RTP-Streams in einem Audio-Player-tauglichen Format. Sprache, die unverschlüsselt im WLAN übertragen wird, kann also problemlos aufgezeichnet und abgespielt werden.

5.2 Verhalten bei Wechsel der Funkzelle

Das Cisco 7920 WLAN-Handset implementiert ein auf die Sprachübertragung optimiertes Handover-Verfahren. Basis ist die kontinuierliche Bewertung des RSSI und das regelmäßige Scanning der WLAN-Kanäle. Hierzu werden die Kanäle in drei Klassen eingeteilt:

- Klasse 1 „Verfügbare Kanäle bzw. aktueller Kanal“: Dies sind Kanäle, auf denen das 7920 die Anwesenheit eines Access Points festgestellt hat. Diese Kanäle und die zugehörigen Access Points können auf dem 7920 angezeigt werden, wie in Abbildung 14 gezeigt. Ein Scanning erfolgt auf diesen Kanälen alle 2 Sekunden.

- Klasse 2 „Überschneidungsfreie Kanäle (non-overlapping channels)“: Dies sind Kanäle, die mindestens fünf Kanäle (und damit mindestens 25 MHz) vom aktuell verwendeten Kanal entfernt sind. Wird beispielsweise auf Kanal 7 operiert, so werden die Kanäle 12, 13, 1 und 2 als überschneidungsfrei eingestuft. Ein Scanning erfolgt auf diesen Kanälen alle 6 Sekunden.

- Klasse 3 „Kanäle mit Überschneidung (overlapping channels)“: Dies sind entsprechend Kanäle, deren Abstand zumaktuell verwendeten Kanal unter 25 MHzliegt. Wenn Kanal 7 aktuell verwendet wird, so sind die Kanäle 3 bis 6 und 8 bis 11 in diese Kategorie eingeordnet. Ein Scanning erfolgt auf diesen Kanälen alle 60 Sekunden.

Das Scanning erfolgt auf den einzelnen Klassen mit unterschiedlicher Häufigkeit. Hintergrund ist folgender: In Klasse 1 ist die unmittelbare Nachbarschaft des Clients eingeordnet. Bedingt durch die Mobilität des Clients (man unterschätze nie die Häufigkeit eines Zellwechsels bei Schrittgeschwindigkeit in einer Indoor-Umgebung) kann es hier schnell zu Änderungen kommen. In Klasse 2 sind bei einer klas-

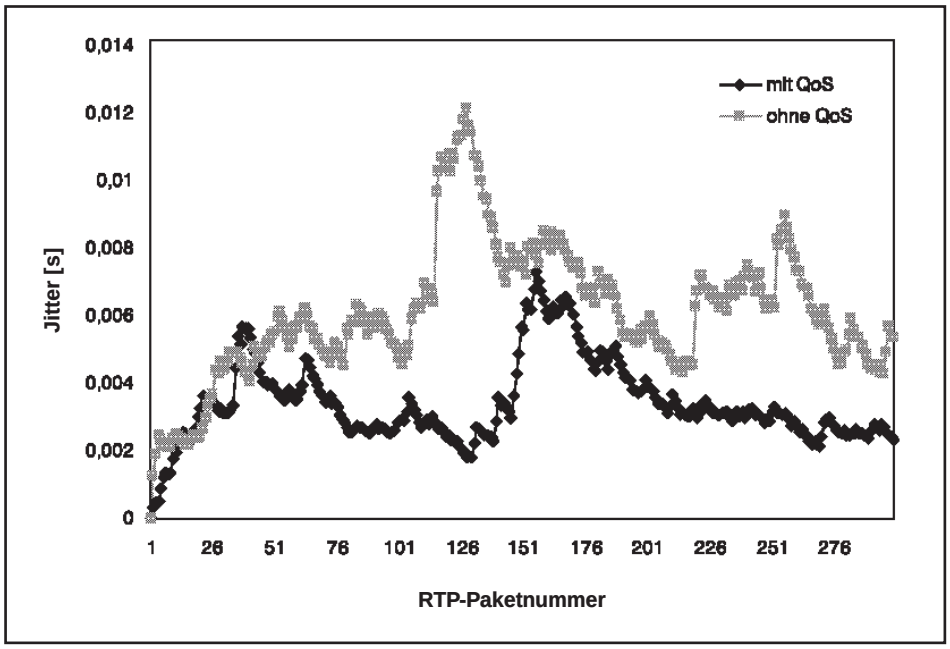


Abbildung 13: Jitter zum 7920 Handset im Vergleich

Report zum Thema

Wireless LAN Evaluierung:

Arbeitsweise, Varianten, Schwachstellen, Planung, Installation

Dieser Report führt Sie umfassend und systematisch in die Wireless LAN-Technik ein. Er zeigt Ihnen, welche gewaltigen Potenziale sich in dieser Technologie verbergen. Er erklärt aber auch, was Sie tun müssen, um diese Technologie erfolgreich unter Vermeidung der typischen Fehler zum Einsatz zu bringen.

Wireless LAN Evaluierung
Januar 2004
449 Seiten
Preis: 398,-- zzgl. MwSt.

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

sischen Zellplanung, die in benachbarten Zellen nach Möglichkeit unterschiedliche Kanäle aus der Menge {1, 7, 13} für Europa bzw. {1, 6, 11} für den FCC-Raum konfiguriert hat, die weiter entfernten Access Points zu suchen. Da erwartet wird, dass es etwas länger dauert, bis diese Funkzellen relevant werden, wird das Scanning hier mit einer etwas niedrigen Frequenz durchgeführt. In der Klasse 3 sollten eigentlich keine Access Points gefunden werden, da hier Nachbarkanalstörungen auftreten können. Da das 7920 für alle erlaubten Konfigurationen funktionieren muss, werden auch diese Kanäle einem Scanning unterzogen, aber eben mit einer sehr geringen Häufigkeit.

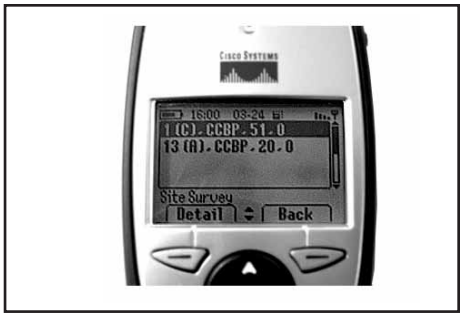


Abbildung 14: Anzeige der verfügbaren („A“ für available) und des aktuellen („C“ für current) Kanals am Cisco 7920

Durch die Eingabe spezieller Keyboard-Sequenzen kann der Nutzer andere Scanning-Häufigkeiten für die drei Klassen bestimmen.

Auf diese Weise unterhält das 7920 eine geordnete Liste von Access Points, die als potentielle Kandidaten für ein Handover in Frage kommen. Angenommen ein 7920 Handset sei an einem Access Point x assoziiert. Das Handset führt einen Handover aus, wenn ein Access Point y existiert, für den gilt $RSSI(x)+15 \geq RSSI(y)$. Weiterhin sucht das Handset nach einem anderen Access Point sobald der RSSI von x unter 20 fällt.

Es ist einleuchtend, dass dieses Verfahren es erfordert, dass Funkzellen eine genügend hohe Überlappung haben, damit beim Übergang von einer Zelle zur anderen frühzeitig der entsprechende neue Access Point bekannt ist.

Bei einer schwachen Überlappung der Funkzellen (die für eine klassische Datenkommunikation vollständig ausreichen mag) kann es passieren, dass man den Überlappungsbereich der beiden Funkzellen bereits passiert hat, bevor im Rahmen des 6-Sekunden-Takts (Klasse 2) der neue Access Point erkannt worden wäre und im 2-Sekunden-Takt (Klasse 1) weiter verfolgt würde. Die Konsequenz wäre ein unter Umständen spürbarer Aussetzer im Gespräch.

Ergänzend sei noch bemerkt, dass das 7920 WLAN-Handset in der Default-Einstellung mit 20 mW sendet. Falls im WLAN die Access Points mit deutlich stärkerer Leistung senden, kann es passieren, dass zwar das 7920 einen Access Point sehr gut empfängt, es aber in der umgekehrten Richtung zu Störungen kommen kann. Die Sprachqualität kann dann in einer Richtung noch als gut empfunden werden, während in der anderen Richtung eine schlechte Qualität festgestellt wird. In dieser Situation muss die Sendeleistung am Handset erhöht werden (was die Akkulaufzeit natürlich entsprechend senkt) bzw. durch zusätzliche Access Points eine bessere Abdeckung bei niedrigerer Sendeleistung erreicht werden. Für weitere Informationen zur Konfigurierung siehe [4].

Zur Bewertung des Handover-Verhaltens des Cisco 7920 haben wir zunächst einen Aufbau vorgenommen, der einen genügend großen Überlappungsbereich zwischen den Funkzellen zusichert (siehe Abbildung 15). Ein Access Point war auf Kanal 1 konfiguriert, der andere auf Kanal 13. Der gezeigte Weg wurde mit dem Cisco 7920 sowie zwei Protokollanalysatoren (Notebooks mit einem NAI Sniffer) abgeschritten. Der eine Analysator zeichnete Kanal 1 auf und der andere Kanal 13. Die Ergebnisse wurden anschließend mit Ethereal analysiert. Abbildung 16 zeigt die gemessene Entwicklung der RTP-Sequenznummern auf Kanal 1 und Abbildung 17 die Aufzeichnung auf Kanal 13. Deutlich sind die Sprünge zu erkennen,

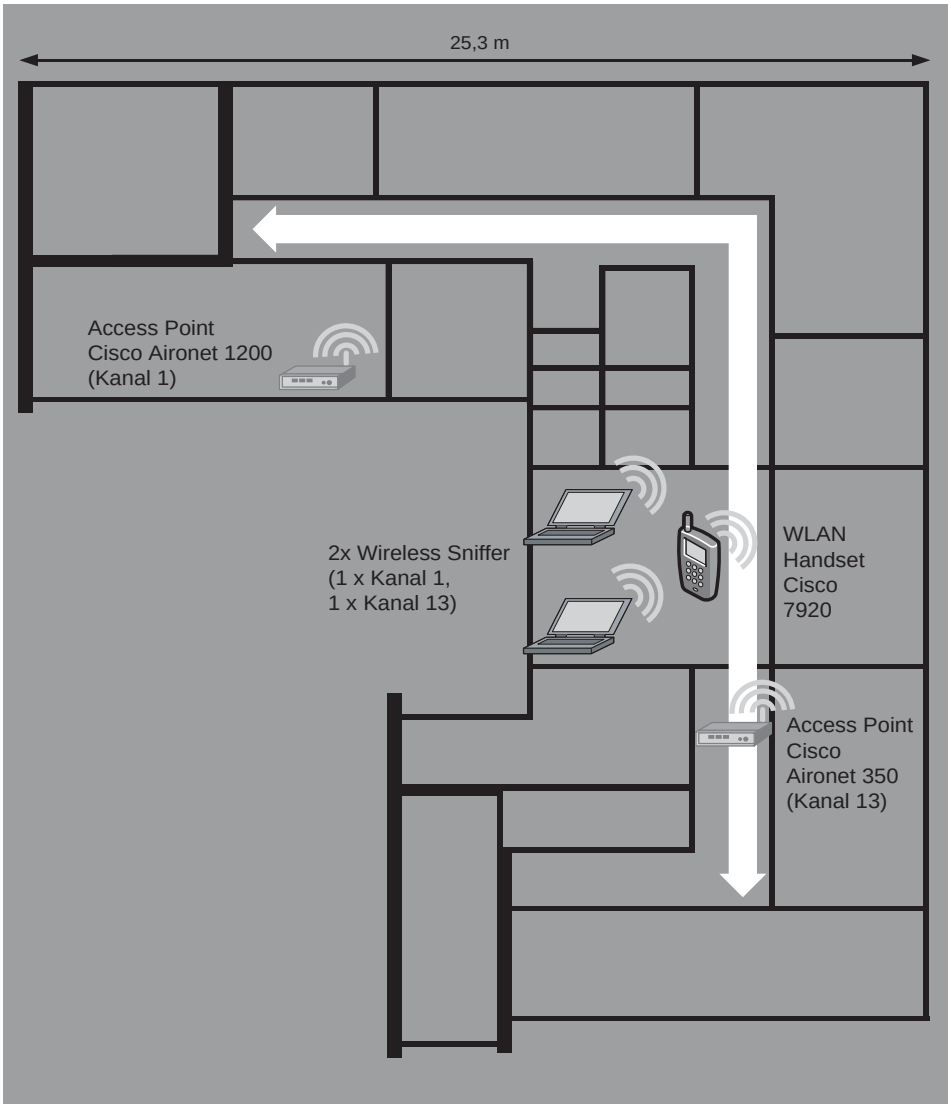


Abbildung 15: Aufbau zum Test des Handover-Verhaltens

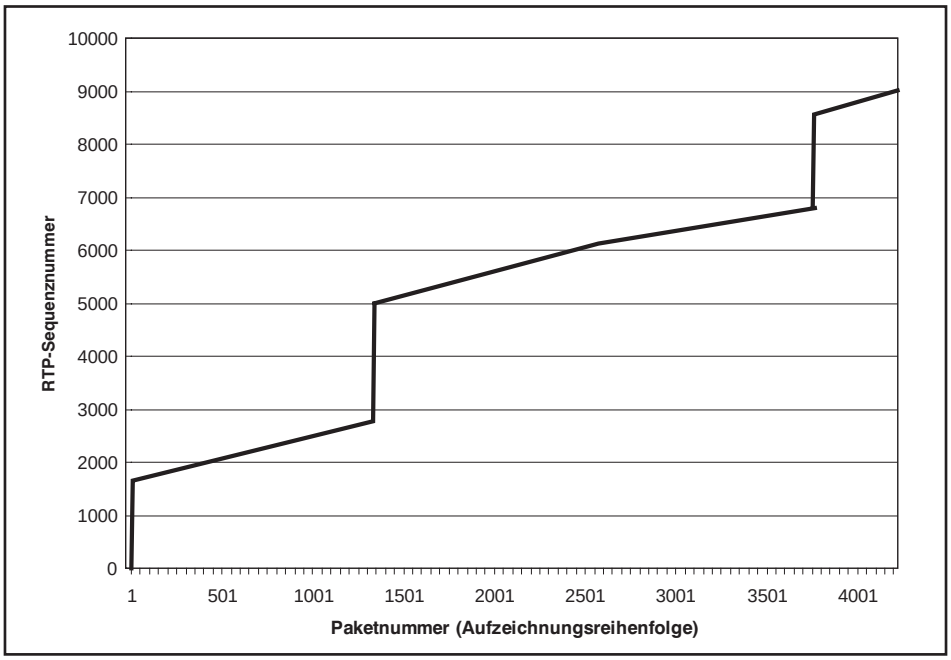


Abbildung 16: Aufzeichnung der RTP-Pakete auf Kanal 1

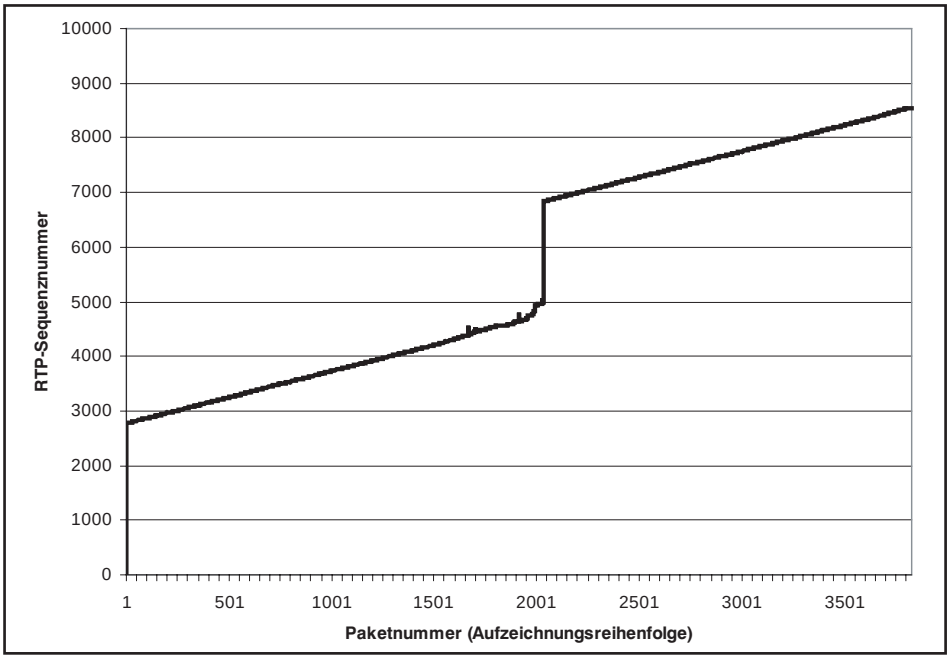


Abbildung 17: Aufzeichnung der RTP-Pakete auf Kanal 13

an denen ein Handover durchgeführt wird.

Bis ca. RTP-Sequenznummer 2.800 befindet sich das Telefon in der ersten Zelle (obere Grafik), dann wechselt es zur zweiten Zelle (untere Grafik), wo es bis ca. RTP-Sequenznummer 5.000 bleibt. Dann wechselt er in die erste Zelle zurück, bleibt dort bis ca. RTP-Sequenznummer 6.800 etc.

Betrachtet man diese Sprünge genauer, so stellt man fest, dass bei einem Zellwechsel RTP-Pakete verloren gehen. Eine genügend große Zahl von Verlusten wird als Aussetzer registriert. Tabelle 1 zeigt die gemessenen Verluste bei einem Zellwechsel als Differenz der zuletzt in der alten Zelle empfangenen Sequenznummer und der als erstes in der neuen Zelle wieder empfangenen Sequenznummer. Es lohnt sich dabei etwas genauer in einen Zellwechsel hineinzuschauen, da nicht nur die Differenz zwischen der Sequenznummer des letzten Pakets in der alten Zelle zum ersten Paket in der neuen Zelle zählt. Bereits vor dem eigentlichen Handover kommt es zu einer Verschlechterung des Funkkanals, der sich in Neuübertragungen auf der MAC-Ebene auswirken kann. Der Protokollanalysator kann dabei durchaus mehrere Übertragungsversuche für ein und dasselbe RTP-Paket aufzeichnen. Solche Neuübertragungen führen zu einer Vergrößerung von Delay und Jitter. Abbildung 18 zeigt den genaueren Blick in die Zeit vor dem Handover Nr. 4, welches ja gemäß Tabelle 1 scheinbar sehr schnell vonstatten ging.

Auf den ersten Blick sehen diese Ergebnisse sehr zufriedenstellend aus. Zu beachten ist jedoch, dass wir diese Handover-Zeiten in einem gewissen Sinne unter besonders günstigen Bedingungen gemessen haben, denn wir haben auf eine Verschlüsselung und eine Authentifizierung (etwa mit LEAP) verzichtet. Während die Verschlüsselung an den Handover-Zeiten nichts ändert, muss die Authentifizierung kritischer betrachtet werden.

Subjektiv hat die Sprachqualität beim Zellwechsel nicht nennenswert gelitten. Der

	Handover 1	Handover 2	Handover 3	Handover 4
RTP-Sequenznummer bei Austritt aus alter Funkzelle	2766	4979	6801	8550
RTP-Sequenznummer bei Eintritt in neue Funkzelle	2773	4990	6833	8553
Anzahl verlorener RTP-Pakete	6	10	31	2
Dauer in Sekunden (bei 20 ms zwischen RTP-Paketen)	0,12	0,2	0,62	0,04

Tabelle 1: Gemessene Dauer einer Gesprächsunterbrechung bei einem Handover

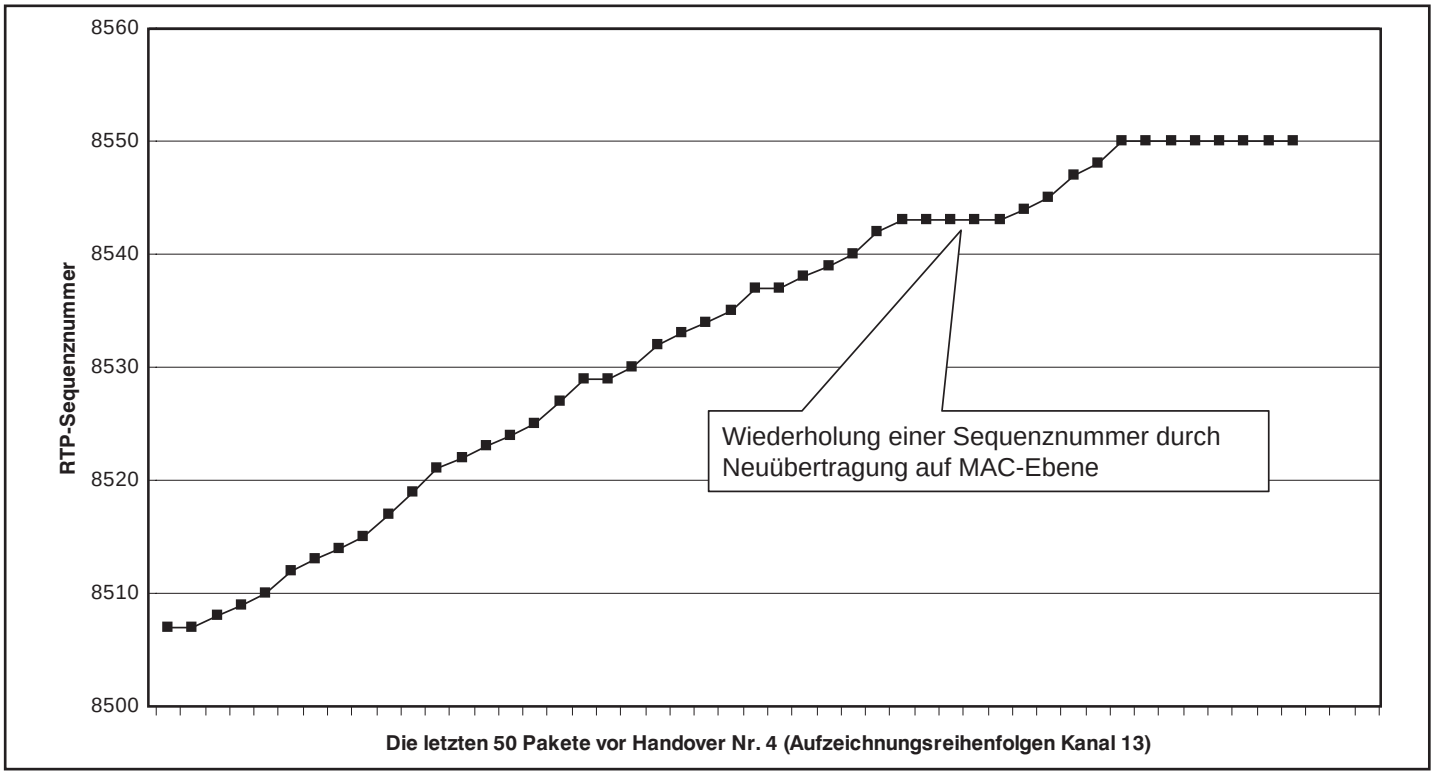


Abbildung 18: Genauere Betrachtung eines Handovers

eigentliche Zellwechsel war im schlimmsten Fall als kaum wahrnehmbarer Aussetzer registriert worden. Ansonsten spürte man den Zellwechsel nur durch eine geringfügige Verschlechterung der Sprachqualität, die nur einen sehr kurzen Moment andauerte.

Vergrößert man jedoch den Abstand zwischen den Access Points geringfügig, kann sich das Bild deutlich wandeln. Wir haben beispielsweise in einer Versuchsreihe die Access Points so verschoben, dass nur eine geringe Überlappung zwischen den Funkzellen gegeben war. Dieser Überlappungsbereich zwischen den Funkzellen wurde auch bei Schrittgeschwindigkeit so schnell passiert, dass der implementierte Handover-Algorithmus nicht schnell genug mitkam. Als Resultat konnten wir Zeiten messen, in denen keine Sprachverbindung mehr bestand, die zwischen 1,2 Sekunden und 3,4 Sekunden lagen. Interessant ist jedoch, dass zwar Gesprächsunterbrechungen der genannten Dauer festgestellt wurden, die Sprachverbindung sich aber stets wieder „berappelt“ hat und kein neuer Anruf getätigt werden musste. Die genannten Zeiten sind natürlich nicht überraschend und das betrachtete Szenario würde man in der Praxis kaum so realisieren. Es soll lediglich darauf hindeuten, dass nicht jede Zellplanung automatisch für die Übertragung von Sprache geeignet ist und gegebenenfalls eine höhere Dichte von Access Points installiert werden muss.

6. Statt einer Zusammenfassung: Planungsaspekte

Die durchgeführten Messungen haben gezeigt, dass die Priorisierung des Verkehrs auf der Luftschnittstelle tatsächlich den gewünschten Effekt für die Sprachübertragung hat und insgesamt, dass VoIP over WLAN technisch das Prototypenstadium verlassen hat und professionelle Lösungen am Markt sichtbar werden. Nun fehlt nur noch die Verabschiedung von IEEE 802.11e und die Verfügbarkeit von entsprechenden Produkten. Dieser Schritt scheint allerdings nicht mehr weit zu sein.

Zur Planung von VoIP-fähigen WLAN und speziell für den nach dem Stand der Dinge zu erwartenden Einsatz von IEEE 802.11e kann momentan folgendes empfohlen werden:

- Es sollten nur zwei bis maximal drei Verkehrsklassen unterschieden werden:
  - Hohe Priorität: Sprachübertragung
  - Mittlere Priorität: betriebliche Anwendungen, die gute Antwortzeiten benötigen (falls vorhanden bzw. zu erwarten)
  - Niedrige Priorität: alle anderen Anwendungen
- Der Verkehr hoher Priorität sollte auf Voice beschränkt werden.
- Die Funkzellen sollten sich vergleichsweise stark überlappen, damit ein Zellwechsel möglichst reibungslos (d.h. schnell) geschehen kann. Dabei sollte die Überlappung der Funkzellen so gestaltet sein, dass an jedem Punkt einer Funkzelle mindestens ein anderer Access Point gut empfangen werden kann.
- Weiterhin sollten die Funkzellen so dimensioniert sein, dass die Anzahl der VoIP-Nutzer in einer Funkzelle das Medium nicht monopolisieren können.
- Die Sendeleistung zwischen Access Points und zwischen VoIP-Handsets muss so abgestimmt sein, dass es möglichst nicht zu einer asymmetrischen Übertragungsqualität (d.h. gute Sprachqualität in die eine Richtung, schlechte Qualität in die andere Richtung) kommen kann.

Generell gilt, dass eine bereits bestehende Installation in einem Site Survey zunächst auf ihre VoIP-over-WLAN-Fähigkeit überprüft werden muss. Gegebenenfalls müssen alleine aus Handover-Gründen Access Points nachgerüstet werden, um eine bessere Überlappung der Funkzel-

len sicherzustellen. Dies kann natürlich im gesamten Funknetz eine Neuplanung der Kanalzuordnung nach sich ziehen.

Genaue Abschätzungen für die Dimensionierung der Funkzellen sind zur Zeit noch schwierig. Als eine erste Daumenregel kann angesetzt werden, dass pro Funkzelle nicht mehr als vier parallele VoIP-Übertragungen stattfinden sollten, damit anderen Anwendungen noch genügend Raum gelassen wird. Dies bedeutet bei einem konservativen Gleichzeitigkeitsfaktor von 5, dass sich in einer Zelle nicht mehr als 20 assoziierte VoIP Clients aufhalten sollten.

Bei IEEE 802.11a/h sind in Abhängigkeit der betriebenen anderen Anwendungen durchaus höhere Verkehrsintensitäten möglich, da der 5-GHz-Bereich für VoIP over WLAN einige Vorteile bietet. Zunächst ist mit weniger Störeinflüssen durch Fremdsysteme zu rechnen, da dieser Bereich für die Datenkommunikation ausschließlich von WLAN benutzt werden darf. Außerdem erlaubt das zugewiesene Spektrum (für ein System, das IEEE 802.11h bzw. Dynamic Frequency Selection und Transmit Power Control unterstützt) mit seinen 19 überschneidungsfreien Kanälen den flexiblen Aufbau stark überlappender Funkzellen ohne Interferenzen zwischen Funkzellen auf dem gleichen Kanal zu riskieren.

Es ist daher schade, dass (zumindest aktuell) noch keine VoIP-Handsets angeboten werden, die IEEE 802.11a und IEEE 802.11h unterstützen. Alle bekannten am Markt verfügbaren Produkte setzen auf IEEE 802.11b auf. Für IEEE 802.11g klafft also ebenfalls eine Lücke.

Nun könnte man argumentieren, dass VoIP keine bandbreitenintensive Applikation ist, und dass die Sprachübertragung mit den netto maximal 6 MBit/s in einer Funkzelle nach IEEE 802.11b gut auskommt. Außerdem ist IEEE 802.11b (noch) der dominierende Standard. Andererseits werden hier automatisch Nachteile für eine Migration zu IEEE 802.11g geschaffen, denn der Mischbetrieb zwischen IEEE 802.11g und IEEE 802.11b führt zu erheblichen Leistungseinbußen [1].

7. Literatur

[1] ComConsult Research, “Wireless LAN Evaluierung – Arbeitsweisen., Varianten, Schwachstellen, Planung, Installation”, 2004.

[2] ANSI/IEEE Std 802.11, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999.

[3] IEEE 802.11 WG, “Draft Supplement to IEEE Standard 802.11-1999: Medium Access Control (MAC) En-hancements for Quality of Service (QoS)”, IEEE 802.11e/D5.0, 2003.

[4] Cisco White Paper, “Cisco Wireless IP Phone 7920 Deployment Recommendations”, Version 1.0, 12. März, 2004.

[5] ETSI TS 101 948, “Digital Enhanced Cordless Telecommunications (DECT); DECT derivative for implementation in the 2,45 GHz ISM Band (DECT-ISM)”, V1.1.1, April 2001.

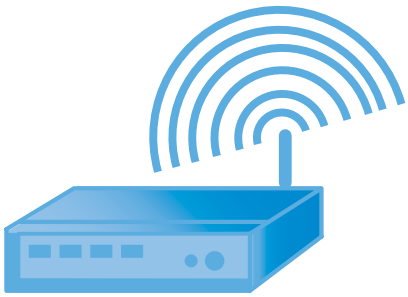
[6] ETSI TS 101 761-1, „Broadband Ra-dio Access Networks (BRAN); HIPER-LAN Type 2; Data Link Control (DLC) Layer, Part 1: Basic Data Transport Functions“, 2000.

[7] Lindgren et al: “Quality for Service Schemes for IEEE 802.11 Wireless LANs – An Evaluation”, Kluwer Academic Publishers (Niederlande), “Mobi-le Networks and Applications”, Ausgabe 8/2003, Seite 223 bis 235.

8. Abkürzungen

AIFS	Arbitration IFS
CRC	Cyclic Redundancy Code
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
CW	Contention Window
DCF	Distributed Coordination Function
DECT	Digital Enhanced Cordless Telecommunications
DIFS	DCF IFS
EDCF	Enhanced DCF
FCC	Federal Communications Commission
FEC	Forward Error Correction
HCF	Hybrid Coordination Function
HIPERLAN	High Performance Radio LAN
IAPP	Inter Access Point Protocol
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter Frame Spacing
MAC	Medium Access Control
MIB	Management Information Base
PCF	Point Coordination Function
QoS	Quality of Service
RSSI	Received Signal Strength Indication
RTP	Real-Time Transport Protocol
RTS	Request to Send
SIFS	Short IFS
SOHO	Small Office Home Office
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
VoIP	Voice over IP

Seminar zum Thema



Wireless LAN Planung, Produktauswahl, Installation, Trouble Shooting

03.05. - 07.05.04 in Zürich-Glattbrugg

14.06. - 18.06.04 in Bonn

12.07. - 16.07.04 in Köln

20.09. - 24.09.04 in Bonn

15.11. - 19.11.04 in Köln

Dieses Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur.

Referenten: Dr. Simon Hoff, Dipl.-Ing. Hans Peter Mohn, Dr.-Ing. Joachim Wetzlar
Einzelpreis: € 2.290,- zzgl. MwSt.

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

CCNE

ComConsult Certified Network Engineer

Lokale Netze
19.04. - 23.04.04 in Aachen
14.06. - 18.06.04 in Aachen
27.09. - 01.10.04 in Aachen
06.12. - 10.12.04 in Aachen

Internetworking
19.04. - 23.04.04 in Aachen
21.06. - 25.06.04 in Aachen
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen

TCP/IP und SNMP
03.05. - 07.05.04 in Berlin
05.07. - 09.07.04 in Bonn
27.09. - 01.10.04 in Berlin
06.12. - 10.12.04 in Bonn

Ethernet Technologien - neuester Stand
28.06. - 02.07.04 in Aachen
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen

Paketpreis für alle vier Seminare € 7.780.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
26.04. - 30.04.04 in Aachen
05.07. - 09.07.04 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
10.05. - 14.05.04 in Aachen
06.09. - 10.09.04 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
21.06. - 25.06.04 in Aachen
27.09. - 01.10.04 in Aachen

Paketpreis für alle drei Seminare mit Etherreal
in Kombination mit Fluke Nettool
€ 7.500.-- zzgl. MwSt. (Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I:
Von den Einzelbausteinen zur integrierten Lösung
03.05. - 07.05.04 in Zürich-Glattbrugg
24.05. - 28.05.04 in Köln
05.07. - 09.07.04 in Bonn
11.10. - 15.10.04 in Bonn

Sicherheitslösungen II:
IP-VPNs, der Kern einer Sicherheits-Infrastruktur
28.06. - 30.06.04 in Köln
13.09. - 15.09.04 in Köln
15.11. - 17.11.04 in Köln

Sicherheitslösungen III:
19.04. - 23.04.04 in Aachen
19.07. - 23.07.04 in Aachen
04.10. - 08.10.04 in Aachen
06.12. - 10.12.04 in Aachen

Paketpreis für alle drei Seminare
€ 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

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

Impressum

Verlag:
Dr. Suppan International institute b.v
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber und verantwortlich im Sinne des Presserechts: Dr. Jürgen Suppan

Chefredakteur: Dr. Jürgen Suppan

Erscheinungweise: Monatlich, 12 Ausgaben im Jahr

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen

Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages

© Dr. Suppan International Institute b.v.