ComConsult Research

Der Netzwerk Insider

November 2005

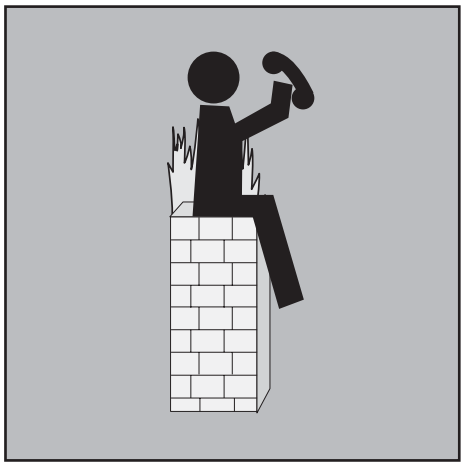
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

VoIP über NAT: Darf's auch etwas mehr sein?

von Markus Schaub

Wer heute einen DSL-Anschluss beantragt, bekommt vielfach eine VoIP-Nummer und einen Router dazu, an den man sein analoges Telefon gleich mit anschließen kann. Vollmundig verspricht die Werbung kostenlose Telefonie innerhalb des Providernetzes, teilweise sogar darüber hinaus zu anderen Anbietern. Auch innerhalb der Unternehmen setzt sich VoIP zunehmend durch. Aber noch handelt es sich um getrennte Welten: ruft man von seinem privaten VoIP-Anschluss aus in einem Unternehmen an, das intern ebenfalls mit VoIP arbeitet, so wird die Sprachübertragung zwischenzeitlich über ein klassisches Telefonienetzwerk übertragen. Damit einher gehen zum einen Kosten für ein



öffentliches Telefonat und zum anderen der Verlust der möglichen Nutzung von Zusatzanwendungen, wie sie über VoIP-Netze möglich sind. Anders formuliert: aktuell besteht die VoIP-Telefonie aus Insellösungen, die über die klassische Telefonie miteinander verbunden werden. Es ist nur eine Frage der Zeit, bis diese Inseln zusammenwachsen. Technisch stellt die Sicherheitsverantwortlichen dieser Prozess jedoch vor An- und Herausforderungen, die von denen, wie sie bislang existierten, erheblich abweichen.

weiter auf Seite 19

Zweitthema

Wireless LAN Marktumfrage

von Dr. Jürgen Suppan

Wireless-LANs müssen sich in den nächsten Jahren mehreren gravierenden Neuerungen stellen. Diese schaffen einerseits neue Potenziale, andererseits aber werfen sie Fragen nach der Invesitionssicherheit und einer langfristig angelegten Weiterentwicklung bestehender WLAN-Netzwerke auf:

- Mit IEEE 802.11n kommt 2006 ein neuer Wireless-Standard, mit den ersten Produkten basierend auf der Vorspezifikation des Enhanced Wireless Consortiums ist im ersten Halbjahr zu rechnen. Er wird im Wesentlichen höhere Datenraten bis zu 600 Mbit/s bieten (resultierende Nutzdatenrate voraussichtlich ca. 240 Mbit/s) und ggf. bei niedrigen Datenraten die Reichweiten erhöhen.
- Mit IEEE 802.16 kommt eine völlig neue Wireless-Technologie, die über eine sehr hochwertige Funktechnik und vor allem eine Maschentopologie verfügen wird. Auf dieser Basis wird der Aufbau redundanter Wireless-Backbone-Strukturen möglich (erste Provider-Lösungen sind bereits im Aufbau). 802.16 arbeitet auch an einer Client-Version (802.16e), doch wird diese frühestens 2007 kommen. Für den Einsatz in normalen Unternehmensumgebungen wird diese Client-Version gegenüber 802.11n wahrscheinlich auch zu spät kommen

weiter auf Seite 7

Top Veranstaltung

ComConsult Winterschule 2005

auf Seite 4

Zum Geleit

Sicherheit in der IP-Telefonie?

auf Seite 2

Report des Monats

Komplett überarbeitet: Wide Area Networks

auf Seite 14

Zum Geleit

Sicherheit in der IP-Telefonie?

Die Diskussion der Sicherheit von IP-Telefonie gehört zu den Mode-Erscheinungen des Jahres 2005. In den letzten Wochen ist sie weiter eskaliert. Dabei muss festgestellt werden, dass in vielen Fällen ein Sicherheits-Niveau gefordert wird, das es für die traditionelle Telefonie so nie gegeben hat. Trotzdem macht die Diskussion Sinn, da sie unter anderem klarstellt, dass jeder, der IP-Telefonie einführen will, auch ein dazu gehörendes Sicherheits-Konzept benötigt.

Eine gute und sachliche Basis für die Diskussion bietet die gerade vom BSI veröffentlichte „VoIPSEC“-Studie. Die entscheidende Aussage dieser Studie liegt aus meiner Sicht allerdings nicht im direkten VoIP-Bereich. Vielmehr macht die Studie klar, dass es keine IP-Telefonie-Sicherheit ohne IT- und Netzwerk-Sicherheit geben kann, da diese Technologien aufeinander aufbauen. Dabei wird auch deutlich, dass sich ein umfassendes Sicherheitskonzept weniger in den hoch stehenden Technologie-Funktionen (Intrusion Detection, ...) ausdrückt als vielmehr in einer alltagstauglichen Basis-Sicherheit.

Als Beispiel soll die folgende Auflistung wichtiger Sicherheits-Maßnahmen dienen, ohne die auch keine Sicherheit für IP-Telefonie erreicht werden kann:

- Sicherheit der Kabelwege: wie einfach ist in Ihrem Unternehmen der Zugang zu Kabeln? IP-Telefonie kann mit einen Zugang zu Kabeln leicht abgehört werden (Etherreal oder Vomit), auch eine SRTP-Verschlüsselung macht wenig Sinn, wenn der einzusetzende AES-Schlüssel zuvor im Klartext übertragen wird

- Sicherheit der Verteilerräume: wie einfach ist der Zugang zu Verteilerräumen und aktiven Netzwerk-Komponenten? Ist es wirklich sicher gestellt, dass Unbefugte keinen Zugang zu Verteiler-Räumen haben? Dies ist der Mega-GAU eines jeden Sicherheits-Konzepts. VLAN-Strukturen können ausgehebelt werden, Netzwerk-Komponenten ausgetauscht werden, eine neue IP-Middleware (ARP, DHCP, DNS) kann installiert werden, die Liste ist beliebig lang. Für einen professionellen Angreifer ergibt dies ein gewaltiges Spektrum an Möglichkeiten. Vor allem aber, würde der angegriffene Benutzer gar nicht merken, dass er abgehört wird

- Sicherheit der Serverräume: kann an Angreifer ohne Probleme physikalisch auf Ihre Server, also auch auf Gatekeeper und Gateways zugreifen? Sind diese Systeme von Ihnen gehärtet worden? Wird diese Härtung kontinuierlich auch bei neu gemeldeten Sicherheitslücken des Betriebssystems nachgeführt?

- Layer-2-Sicherheit: haben Sie ein etabliertes Schutzkonzept gegen MAC-Spoofing und MAC-Flooding?

- DNS, DHCP-Sicherheit: wie sind Ihre IP-Middleware-Infrastrukturen abgesichert?

- Client-Sicherheit: wohl ohne Frage der zentrale Knackpunkt jeder aktuellen Sicherheits-Strategie. Wie stark haben Sie Ihre Clients gegen eine Fremdübernahme geschützt? Welchen Sinn macht eine verschlüsselte Übertragung mit SRTP, wenn die Schlüssel auf den Clients gelesen werden können? Wie viele verschiedene Schlüssel werden eingesetzt?

- Zugang zum Netzwerk: Kann ein Angreifer durch Man in the Middle Angriffe Daten mitlesen oder diese manipulieren?

Die Liste kann beliebig fortgesetzt werden. Bei näherer Betrachtung befasst sich kein einziger der aufgeführten Punkte direkt mit der Sicherheit von IP-Telefonie. Es ist aber sofort offensichtlich, dass diese Sicherheit nicht erreicht werden kann, wenn die in den Punkten angesprochene Basis-Sicherheit nicht gegeben ist.

Man kann die Situation in einem einfachen Statement zusammenfassen: die Diskussion um die Sicherheit der IP-Telefonie macht alle Versäumnisse der Vergangenheit deutlich. Dabei sind herausragende Punkte:

- Der gesamte Bereich der physikalischen Sicherheit: ein unbefugter Zugang zu Kabeln, Verteilern und Servern ist unter allen Umständen zu verhindern. Wenn der etwas platte Spruch „das moderne RZ ist das Netz“ auch nur halbwegs gilt, dann ist die Konsequenz, dass der physikalische Zugang zur Netzwerk-Infrastruktur den Sicherheits-Maßnahmen traditioneller Rechenzentren unterworfen werden muss: Key-Cards mit Protokollierung, Personenschleusen, Einbeziehung in die Videoüberwachung, systematische Auswertung der hier anfallenden Information. Es muss endlich in den Unternehmen klar werden, dass der Zugang zum Netzwerk den Zugang zu Daten ermöglicht, und zwar genau zu den Daten, die man früher Bombensicher im wahrsten Sinne des Wortes geschützt hat

- Schlüssel-Management: die Verschlüsselung der IP-Telefonie ist eine feine Sache und sie ist ohne Frage ein absolutes Muss. Parallel stellt sie einen wesentlichen Fortschritt gegenüber der traditionellen Telefonie dar. Aber: sie erfordert ein geeignetes Schlüssel-Management

- Client-Zugang zum Netz: eine ganze Liste von möglichen Angriffen kann nur verhindert werden, wenn der unauthorisierte Zugang zum Netzwerk von vornherein unterbunden wird (Angriffe wie MAC-Spoofing, MAC-Flooding entfallen damit). Eine Anmeldung am Netz mit IEEE 802.1X mit daran gebundener Zuweisung von Rechten ist eine unverzichtbare Voraussetzung für die Sicherheit der IP-Telefonie

- Client-Sicherheit: wenn ein Client durch Anmeldung am Netz Rechte erwerben kann und somit frei im Unternehmen agieren kann, muss unter allen Umständen verhindert werden, dass der Client übernommen werden kann. Typische Wege sind hier die Installation gefährlicher Software, eine Attacke basierend auf Schwachstellen des eingesetzten Browsers, eine Attacke über ein Email-Attachment

Sicherheit in der IP-Telefonie?

- Physikalischer Zugang zum Client: wie sicher ist ein Client, wenn jeder Besucher ohne Kontrolle am Client Platz nehmen kann und mit den Rechten des Clients im Netzwerk arbeiten kann (wie in diversen Ministerien, Krankenkassen, Versicherungen, Sparkassen, ... immer wieder zu beobachten)? Smart-Cards oder biometrische Verfahren werden zur absoluten Sicherheit gerade in Publikums-Bereichen unvermeidbar gehören

Wie hoch ist das Gefahrenpotenzial der IP-Telefonie einzuschätzen? Wie wahrscheinlich ist ein Angriff auf dieser Ebene?

- Der wahrscheinlichste Angriff dürfte die Blockade sein, bei der von Außen oder von Innen die Fähigkeit der Telefonie unterbunden wird. Kritisch ist dies primär für die Erreichbarkeit des Unternehmens für Kunden, da die Kommunikation nach Außen auf jeden Fall über Handys aufrecht erhalten werden kann

- Das Abhören von Telefonaten wird sich maximal auf ausgewählte Entscheidungsträger reduzieren. Selbst hier stellt sich aber die Frage, ob die dabei zu erzielende Information nicht auf anderen Wegen einfacher ermittelbar ist. Solange die IP-Telefonie-Installationen gekapselte Insel-Installationen sind, kann ein Abhör-Angriff auch primär nur von Innen erfolgen (je nach Architektur und Handhabung der Standort-Verbindungen)

- Damit sind wir beim Kern des Problems: die kritischen Informationen eines Unternehmens im Sinne der Vertraulichkeit sind die Daten. Jeder Angriff mit dem Ziel der Informations-Gewinnung wird tendenziell hier ansetzen. IP-Telefonie ist maximal ein sekundäres oder ein temporäres Angriffsziel (beispielsweise während Übernahmeverhandlungen)

Ich würde gerade den letzten Punkt noch gerne etwas härter formulieren: wer die Sicherheit von Web-Applikationen auf einem Niveau betreibt, dass im Schnitt 90% aller Web-Applikationen angreifbar sind, der braucht sich um die Sicherheit der IP-Telefonie auf Dauer keine Gedanken zu machen. Das gleiche gilt für die Client-Sicherheit. (Ich verweise auf den Workshop zur Sicherheit von Web-Applikationen, der auf dem ComConsult Sicherheitsforum 2005 durchgeführt wurde. Die hier an realen und nicht speziell veränderten Applikationen vorgeführten Attacken gipfelten in der kompletten Replizierung einer Datenbank; für Interessenten: den Workshop wird es in aktualisierten Form auf dem Sicherheitsforum 2006 wieder geben, bis dahin kann er als Inhaus-Veranstaltung gebucht werden).

Moderne IT-Architekturen mit Standortübergeifenden Geschäftsprozessen benötigen IT- und Netzwerk-Sicherheit. Gerade die Umsetzung von wichtigen Geschäftsprozessen auf IT-Ebene erhöht die Angreifbarkeit von Unternehmen. Speziell mobile Teilnehmer mit Ortsunabhängigem Zugang zu allen relevanten Daten sind ein Sicherheitsproblem der ersten Klasse.

Die Forderung nach der Sicherheit von IP-Telefonie ist nahe liegend. Und sie ist sinnvoll. Spannend ist, dass dabei durchaus ein Sicherheitsniveau erreicht werden kann, das weit über dem der klassischen Telefonie liegen kann. Aber: Voraussetzung für diese Sicherheit ist, dass die Basis-Sicherheit der IT und der zu Grunde liegenden Netzwerke gegeben ist. Hier ist die eigentliche Baustelle.

Ihr
Dr. Jürgen Suppan

Top Winter-Veranstaltung

Winterschule 2005 - Intensiv-Update auf den letzten Stand der Netzwerktechnik Netzwerk-Design im Brennpunkt

Vom 05. - 09. Dezember veranstaltet die ComConsult Akademie ihre diesjährige Winterschule in Aachen.

Netzwerke unterliegen einer permanenten Weiterentwicklung. Vor allem der Wunsch nach Benutzertrennung und nach kürzeren Konvergenzzeiten hat zu starken Änderungen im Backbone-Design geführt. Die Integration von WLANs und IP-Telefonie verändert Netzwerk-Architekturen zusätzlich. Produkte haben sich entsprechend weiter entwickelt. Moderne Switch-Systeme bieten einen deutlichen Zugewinn an Gestaltungsfunktionalität für leistungsstarke und zugleich sichere Netzwerke.

Die Winterschule 2005 greift diese hochaktuellen Entwicklungen auf. Kompakt und intensiv werden die aktuellsten Themen der Netzwerk-Technik innerhalb von 5 Tagen erklärt und analysiert. Die Winterschule 2005 wendet sich an Fortgeschrittene und bietet die optimale Möglichkeit, mit einer Intensiv-Veranstaltung auf den neuesten Stand der Netzwerk-Technik zu kommen.

Die Winterschule 2005 bietet den 5-Tages-Intensiv-Update auf den letzten Stand der

Netzwerk-Technik. Wir haben für Sie die aktuellen Entwicklungen analysiert, Erfahrungen aus Labor und gerade abgeschlossenen Projekten eingearbeitet und daraus eine Auswahl aus den zur Zeit anliegenden Top-Themen getroffen.

Die Winterschule 2005 ist die perfekte Gelegenheit, in 5 Intensiv-Tagen auf den neuesten Stand der Technik zu kommen. Top-Referenten mit hochaktuellen Themen, die ideale Umgebung für umfangreiche Diskussionen und ein herausragender Überblick auf die Entwicklungen der nächsten Monate und Jahre bilden das Fundament für eine unserer besten Veranstaltungen des Jahres 2005.

Einige wichtige Themen in der Übersicht:

- Verändertes Campus-Design und Segmentierung
- Architektonische Einbindung von WLANs
- Konvergente Netzwerke und ihre Konsequenzen
- Quality of Service als Basis einer Verkehrstrennungs-Strategie
- Ausdehnung Layer-3 bis in den Edge-Bereich
- Voice-Ready Netzwerke: was heißt das?
- Sicherheit im Netzwerk und seine praktische Umsetzung
- Wireless-LAN-Technologie neuester Stand

Zur Sicherstellung der Diskussionsfähigkeit und einer interaktiven Kommunikation haben wir die Teilnehmerzahl begrenzt. Zögern Sie deshalb nicht, sich schnell einen Platz in dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Winterschule 2005

Ich buche das Seminar
Winterschule 2005
vom 05.12. - 09.12.05 in Aachen

☐ mit Report „Netzwerkdesign-Wettbewerb 2005“ - Preis von € 2.438,- zzgl. MwSt.
☐ ohne Report „Netzwerkdesign-Wettbewerb 2005“ - Preis von € 2.290,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

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

Programmübersicht - Winterschule 2005

Montag, den 05.12.2005

9:30 - 11:00 Uhr
Neue Netzwerk-Technologien und ihr zukünftiger Einfluss auf das Design und die Nutzung von Netzwerken
- Was sich bei den Anforderungen ändert
  - Mehr Bandbreite und ihre Verwendung
  - Änderungen im Access-Bereich, im Concentrator-Bereich, im Core-Bereich
- Hierarchische Architekturen, LND-Konzept
- Bewertungs-Kriterien für Design und Technologien
- Bewertung von WLAN und Wireless:
  - PAN, LAN, MAN / RAN
- Neue Wireless-Technologien: WiMAX
  - Marktbedeutung
- Verfahren
- Einsatzszenarios
- Produktreife

Dipl.-Inform. Petra Borowka, UBN

ab 11:30 Uhr
Netzwerk-Design im Umbruch, Teil I
- LAN-Redesign
  - Neuerungen im Access Design
  - Neuerungen im Campus-Design
  - Senkung der Konvergenzzeiten: neue Verfahren in der Übersicht
  - Neue Management Möglichkeiten: IEEE 802.1AB LLDP, ANSI/TIA-1057 LLDP-MED
- Erweiterte Integrations-Aufgaben und ihre strukturelle Lösung
  - WLAN-Integration: Flächenkonzepte
  - WLAN-Integration: WLAN Switching und WLAN-Controller
  - WLAN-Integration: CAPWAP

Dipl.-Inform. Petra Borowka, UBN

11:00 - 11:30 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, den 06.12.2005

9:00 - 10:30 Uhr
Netzwerk-Design im Umbruch, Teil II
- Erweiterte Integrations-Aufgaben und ihre strukturelle Lösung
  - Voice-Integration
  - Resultierender Einsatz von QoS
  - Resultierende Anforderungen für Sicherheit
  - Zonen und Sicherheits-Konzepte
- Struktur und Empfehlungen für ein Redesign
  - Strukturbausteine
  - Wesentliche Design-Regeln

Dipl.-Inform. Petra Borowka, UBN

11:00 - 15:00 Uhr
Der ComConsult Research Netzwerkdesign-Wettbewerb
- Vorgegebenes Szenario
- Design-Alternativen der Hersteller
- Analyse: welche Verfahren liegen im Trend
- Analyse: wie ändern sich Switch-Produkte
- Vorstellung der besten Designs und herausragender Design-Elemente
- Zusammenfassung und Bewertung
- Empfehlungen für die Teilnehmer

Dipl.-Inform. Petra Borowka, UBN

ab 15:30 Uhr
Sicherheit im Netzwerk: Verfahren, Strategien und Konzepte
- Zugangssteuerung und Rechtezuweisung durch Einsatz von 802.1X
- Weitergehende Konzepte: Bildung virtueller Benutzergruppen
- Trennung von PC und Telefon
- Varianten der Trennung von Vertrauensbereichen: VLAN, Virtuelle Router und ACL in der vergleichenden Analyse
- Verschlüsselung Ende-zu-Ende: ist das machbar?
- Intrusion Detection und Prevention: Anomalie-Erkennung und Reaktion
- Sicherheit im WLAN und praxisgerechte Umsetzung

Markus Schaub, ComConsult Technologie Information GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:30 Uhr Kaffeepause

Mittwoch, den 07.12.2005

9:00 - 12:30 Uhr
IP-Telefonie: Produkte, Hersteller, Trends
- Alcatel, Avaya, Cisco und Siemens im Vergleich
- Wohin geht der Trend
- Wo werden wir in 1 bis 3 Jahren stehen
- Wo liegen Grenzen der Entwicklung

Dipl.-Inform. Petra Borowka, UBN

ab 13:30 Uhr
Der zukünftige Mega Standard SIP
- Struktur und Arbeitsweise von SIP
- Testbericht und Erfahrungen mit SIP-Clients und SIP-Servern
- SIP als Basis für Multimedia-Lösungen: Vision oder Realität?
- Problembereich NAT-Traversal
- Empfehlungen und Diskussion

Markus Schaub, ComConsult Technologie Information GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 13:30 Uhr MIttagspause
14:30 - 15:00 Uhr Kaffeepause

Donnerstag, den 08.12.2005

ab 9:00 Uhr
IP-Telefonie-Projekterfahrungen
- IP-Telefonie-Design-Varianten
- Projekterfahrungen: Bewährtes Vorgehen bei Ausschreibungen
- Projekterfahrungen: Mögliche Migrationsalternativen im Vergleich
- Projekterfahrungen: Applikationen und Sonderanwendungen in einer IPT-Umgebung: von Fax bis Sprachaufzeichnung
- Wie Voice-tauglich sind bestehende Netze und wie dies zu verifizieren ist
- Neueste Ausschreibungsergebnisse: wie wirtschaftlich ist IPT?
- Voice im WAN versus Voice über öffentliche Provider-Netzwerke: welcher Weg ist sinnvoller?

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

Netzwerk-Konvergenz und seine Handhabung in der Praxis
- Herausforderung: Integration Sprache, Daten, Video, Produktion, Logistik, Meldetechnik
- Unterschiedliche Anforderungen an Verfügbarkeit, Sicherheit, Leistungsfähigkeit und wie sie zu erfüllen sind
- Wo ist Sicherheit am besten zu implementieren: auf Anwendungs-, auf System- oder auf Netzebene?
- Probleme und Tücken bei Power over LAN
- Anschluss von PC und Telefon am Arbeitsplatz
- Sinnfälligkeit des Einsatzes verschiedener VLAN für verschiedene Anwendungen
- IP-Adresskonzept für Konvergenzszenarien
- Quality of Service im LAN / WAN / WLAN

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

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr MIttagspause
15:00 - 15:30 Uhr Kaffeepause

Freitag, den 09.12.2005

ab 9:00 Uhr
Wireless-Networks im Wandel
- Neue WLAN-Übertragungstechniken: Was von IEEE 802.11n zu halten ist
- Controller-basierte Architekturen und ihre Vorteile
- Wird CAPWAP die bestimmende Standard-Familie für Controller-basierte WLAN?
- Konsequenzen für den Aufbau des Distribution System und der WLAN-Sicherheitsinfrastruktur
- Produktpalette Wireless Switching
- Mobilität und Sicherheit: Wie aufwändig ist IEEE 802.11i?
- Voice im WLAN: Stand der Technik und Ausblick
- WLAN-Planung: Was leisten Planungstools
- Wird die traditionelle Funkzellenplanung angesichts dynamischer Frequenz- und Kanalwahl sowie dynamischer Steuerung der Sendeleistung noch gebraucht?
- WLAN-Management: Die Schwierigkeiten der Analyse und Lokalisierung von Fehlern und Sicherheitsvorfällen auf der Luftschnittstelle

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr MIttagspause
15:00 Uhr Ende der Veranstaltung

Neue Seminarreihe 2006

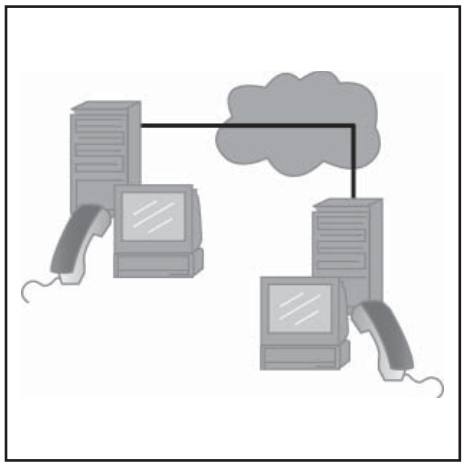
Session Initiation Protocol SIP -
Basis-Technologie der IP-Telefonie

Die ComConsult Akademie veranstaltet vom 13.- 15. Februar 2006 erstmalig ihre neue Seminarreihe „Session Initiation Protocol SIP“ in Köln.

Holiday Inn am Stadtwald in Köln Der größte Nachteil der bisher überwiegend verkauften Produkte für IP-Telefonie ist, dass sie mit Hersteller-spezifischen Protokollen arbeiten. Doch dies ist ein reiner Übergangs-Zustand. Mit dem Session Initiation Protocol hat sich ein Standard etabliert, der die Zukunft der IP-Telefonie ausmachen wird. Schon jetzt sind signifikante Anbieter auf diesen Standard umgeschwenkt, die verbleibenden Anbieter werden das kurz- bis mittelfristig nachholen.

Für Jeden, der sich mit IP-Telefonie auseinander setzt, sind elementare Kenntnisse von SIP unverzichtbar. Dies liegt auch darin begründet, dass der Standard in ständiger Weiterentwicklung ist und zurzeit nicht alle Funktionsbereiche abdeckt, so dass die Hersteller fehlende Funktionen basierend auf SIP ergänzen (was der Standard gestattet).

In diesem Seminar lernen Sie:
- was SIP leistet
- was SIP nicht leistet
- was SIP wann leisten wird
- wo die Vor- und Nachteile gegenüber den bisherigen Lösungen liegen
- wie wichtige Hersteller zu SIP stehen
- wie Sie eine SIP-Lösung aufbauen und erfolgreich zum Laufen bringen
- wie Sie mit NAT-Firewalls umgehen



Zum Inhalt

Motivation
- Trends • Marktverbreitung
- Marktbedeutung • Alternativen
  - Klassische Telefonie
  - H.323
  - Propietäre Lösungen

Grundlagen VoIP
- Komponenten einer VoIP Lösung
- Anforderungen: Durchsatz, Delay, Jitter, QoS, CAC
- Codecs
- Basis-Protokolle: RTP / RTCP

Theorie: SIP
- SIP: Funktionsweise und Protokolle
  - SIP und SDP
  - Lokalisierung, Notruf
  - SIMPLE • SIPPING, SIPPING19
  - Einsatzszenarien
  - Ungelöste Probleme

Mehrwertdienste
- Anwesenheitsdienste
- Video • Kollaboration
  - AS Appl. Sharing (half-, fullduplex)
  - DS Deskt. Sharing
  - WB el. Flipchart

SIP-Anbindung an non-SIP Lösungen

Produkte, Lösungen
- Kriterienliste
- Portfolios (Avaya, Alcatel, Cisco, Nortel, Siemens etc.)
- Server (Asterisk, OpenSource etc.)
- Endgeräte (Symbol, X-ten etc.)
- Kompatibilität (z.B. Basic, Value Add, proprietär etc.)

SIP Demo

Security / NAT
- Motivation • Voraussetzungen
  - IP/UDP
- Authentifzierung
- Verschlüsselung
- NAT
  - ALG • VPN
  - Firewall-Proxys (SIP aware)
  - Propietäre Lösungen
  - STUN • TURN • ICE

Produkte

NAT Demo

Demonstrationen
- Features
  - innerhalb eines Herstellers
  - herstellerübergreifend
- NAT
  - was geht
  - was geht nicht

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Session Initiation Protocol SIP

☐ Ich buche das Seminar
Session Initiation Protocol SIP
vom 13. - 15.02.06 in Köln
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

Wireless LAN Marktumfrage

Fortsetzung von Seite 1

Dr. Jürgen Suppan gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt. Seine Seminare zählen durch ihren didaktischen und lebendigen Aufbau und ihre Praxisnähe und Herstellerneutralität zu unseren erfolgreichsten Veranstaltungen.

- Mit dem Kauf von Airespace hat CISCO Systems eine neue Welle der Wireless-Technik ausgelöst. In den USA prägen Wireless-Switches den Kern der Wireless-Enterprise-Technologie. Wireless-Switches lösen signifikante Probleme der bisherigen Technologie (Management großer Mengen an Access Points, Koordination zwischen Access Points, Layer-3-Roaming), sie sind aber nur für bestimmte Anwendungsbereiche sinnvoll (zum Beispiel werden sie nicht für die typischen Konferenzraum-Versorgungen benötigt)

- Nachdem die Interferenzen im 2,4 GHz-Band immer mehr zunehmen und auch bereits die ersten Konsumer-Produkte in das 5 GHz-Band wechseln, steht nun auch dem Enterprise-Markt dieser Wechsel bevor. Dominierte dieses Frequenzband hier bisher vor allem in Outdoor- bzw. Backbone-Anwendungsbereichen, in denen die hohe Sendeleistung von einem Watt benötigt wurde, so wird sie zunehmend den Standard auf der Client-Seite prägen

- Voice over Wireless wird Standard werden. Mit der Einführung von IP-Telefonie wird man einen Ersatz für die bisherigen DECT-Installationen suchen. Parallel werden neue Handy-Generationen standardmäßig Voice over Wireless unterstützen (siehe Motorola). Damit entstehen neue Herausforderungen, da ein wirklich mobiles Endgerät ins Spiel kommt. Vor allem erfordert dies ein spezielles, Sprach-optimiertes Zellen-Design

- Wireless LANs haben sich zur Mega-Technik im Logistik-Bereich entwickelt. Sei es als Infrastruktur für RFID-Anwendungen oder als Kommunikations-Infrastruktur für Transport-Steuerungen aller Art. Damit halten sie Einzug in den Produktionsbereich. In den letzten Monaten hat sich gerade hier eine sehr hohe Eigendynamik entwickelt. Die Vorteile der Wireless-Technik für Produktion und Logistik sind so groß, dass hier eine hohe Nachfrage entstanden ist

- IEEE 802.11i hat die bestehenden Sicherheits-Probleme gelöst und schafft die Voraussetzungen für eine hochwertige Sicherheits-Infrastruktur, die WLANs zu den sichersten Netzen überhaupt machen

Die sich damit ergebenden Änderungen sind weitgehend. Es ist aber absehbar und auch zu hoffen, dass mit diesen Änderungen ein solides Fundament für eine stabile mehrjährige Nutzung der Technik geschaffen wird.

Angesichts dieser doch erheblichen Veränderungen der Wireless-Technologie stellen sich folgende Fragen:

- Sind Investitionen in Wireless-LANs gerade unter dem Blickwinkel der anstehenden Änderungen sicher? Sollte man nicht auf 802.11n warten? Sind Access Points mit mehreren und vor allem austauschbaren Radioteilen eine Lösung? Bieten Wireless-Switches ggf. den höheren Investitionsschutz?

- Ist die IEEE 802.16-Client-Variante, mit der frühestens in 18 Monaten zu rechnen ist, mit der Einführung von 11n bereits vor ihrer Geburt gestorben? Lohnt sich das Warten auf 802.16-Backbone-Strukturen oder bietet 802.11a/h in Verbindung mit zusätzlichen Redundanzen hier bereits eine ausreichende Leistung?

- Wie stabil ist die Hersteller-Landschaft? Gerade die traditionellen Netzwerk-Hersteller haben sich im Bereich Wireless in den letzten 2 Jahren nicht gerade mit Ruhm bekleckert und diverse Investitionsruinen hinterlassen. Der Wechsel auf Wireless-Switches führt u.a. dazu, dass bei einigen Herstellern ganze Produktserien aussortiert werden. Auf welchen Hersteller sollte man setzen? Bieten spezialisierte Hersteller hier eine höhere Leistung, Stabilität und vor allem Investitionssicherheit?

- Wie lange wird 802.11n gültig sein, was kommt danach? Braucht man vor allem mehr als 11n leistet? Im Endeffekt muss man heute davon ausgehen, dass 11n-Lösungen für mehrere Jahre die normale Installations-Situation darstellen werden. Von daher wird man im Zellendesign eine gewisse Dauerhaftigkeit anstreben. Folge-Technologien wären also vorrangig dann sinnvoll, wenn sie pro Zelle eine höhere Bandbreite bieten und somit eine höhere Teilnehmerzahl gestatten

- Wie kann eine sinnvolle Langzeit-Migrations-Strategie aussehen?

- Werden Wireless-Switches generell die traditionellen Access-Point-Strukturen ablösen? Wie sehen sinnvolle Migrationswege aus?

- Wie weit wird die Einführung von WLANs in den Produktionsbereich gehen? Sind sie wirklich tauglich für diesen Bereich? Welche Sonderfunktionen wird dies erfordern?

- Sind die Anwender wirklich bereit, die in 802.11i festgelegte Infrastruktur aufzubauen oder bleiben sie bei mehr oder weniger angreifbaren Einfach-Lösungen?

Wireless LAN Marktumfrage

- Bietet IEEE 802.11n die technische Basis zur endgültigen Verdrängung der Tertiär-Verkabelung? Auch mit einer Datenrate von 600 Mbit/s entspricht eine Zelle unter Berücksichtigung des Protokoll-Overheads der Kapazität von ca. 3 x 100 Mbit/s Kabelanschlüssen. Damit lassen sich zwischen 10 und 20 Clients mit einer Leistung versorgen, die im statistischen Mittel dem 100 Mbit/s-Kabel entspricht

Die Antworten auf diese Fragen gibt im Wesentlichen der Käufer. Technisch sind ganz verschiedene Entwicklungen denkbar.

Unsere WLAN-Umfrage diente dazu, den aktuellen Markttrend in Deutschland aufzuzeigen. Ziel ist es, einen höheren Grad an Investitionssicherheit zu schaffen. Gleichzeitig sollten die im Rahmen von Wireless-Projekten notwendigen Entscheidungen aufgezeigt werden.

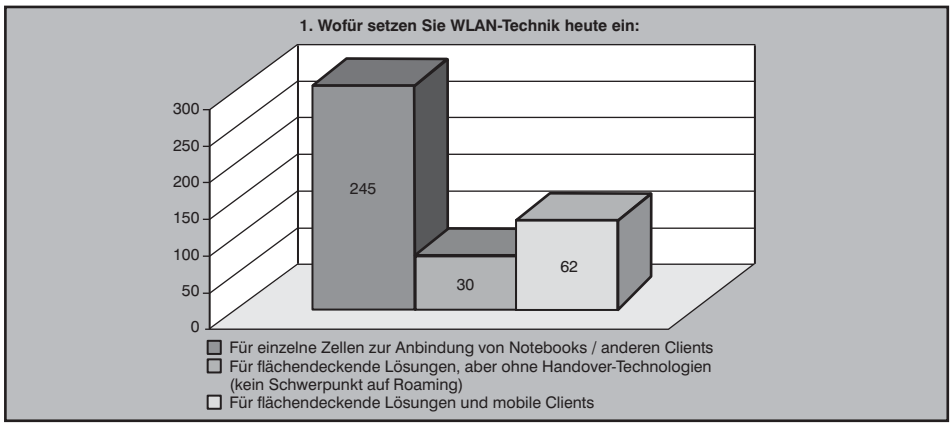
Die Abbildungen rechts und auf den Folgeseiten stellen die gestellten Fragen mit den erhaltenen 306 Antworten dar. Wir haben die Antworten nicht mit statistischen Verfahren auf Signifikanz geprüft, es konnte aber bereits zu einem sehr frühen Zeitpunkt festgestellt werden, dass sich mit weiteren Antworten keine Verschiebungen der Schwerpunkte mehr ergeben haben. Wir gehen deshalb von einer sehr hohen Signifikanz mit relativ niedrigen Schwankungsbreiten aus. Für unsere Untersuchung war es nicht notwendig, in den Antworten die Unternehmensgrößen zu unterscheiden. Hier könnte bezüglich der Signifikanz der Antworten nach Unternehmensgröße ein Abweichungsrisiko bestehen.

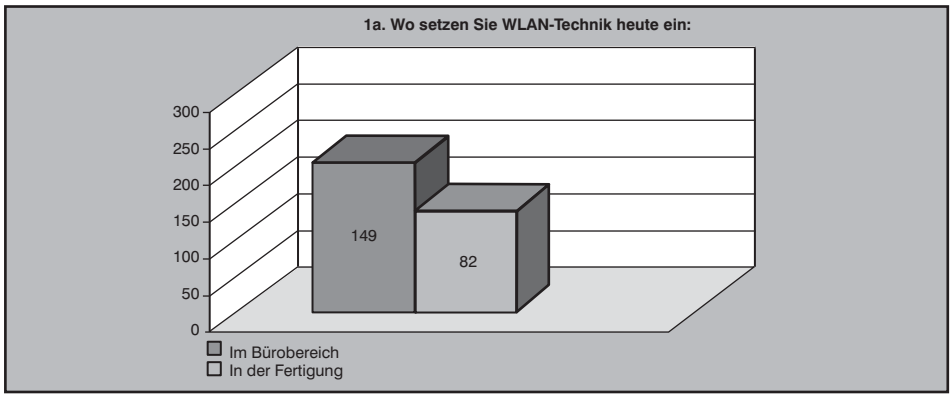
Aus den erhaltenen Antworten leiten wir folgende Schlussfolgerungen und Empfehlungen ab:

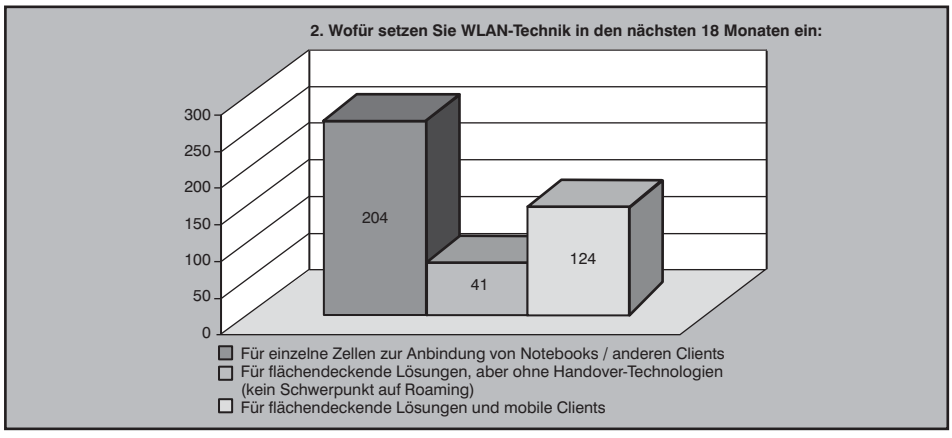
- Bisher dominieren WLAN-Netze vor allem als einzelne Zellen, flächendeckende Lösungen sind noch selten. Es ist aber zu erkennen, dass ein ernstzunehmender Trend zu flächigen Lösungen besteht. Dies wird ein deutliches Umdenken in der Zellplanung erfordern

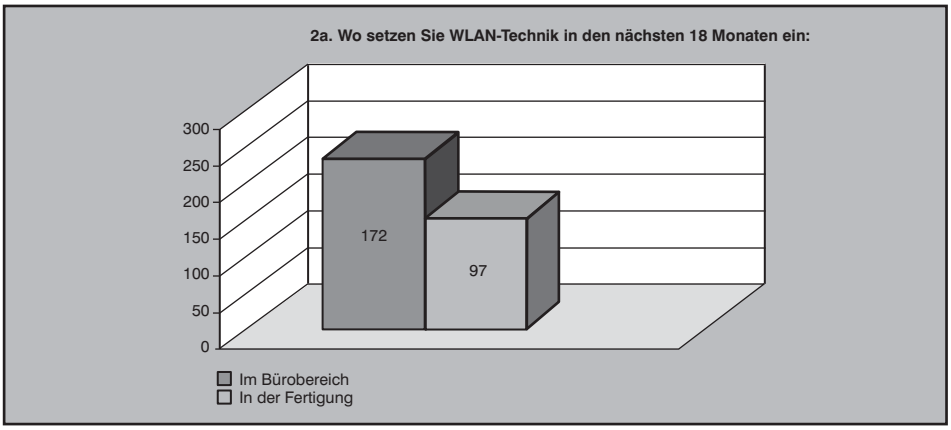
- Vor allem hat sich die Einstellung der Teilnehmer zu Handover und automatischem Zellwechsel (Roaming) geändert. Wurde diese Eigenschaft noch vor einem Jahr nur von wenigen Anwendern gefordert, so haben inzwischen 74,8% der Umfrageteilnehmer diese Anforderung

- Wireless-Switches sind für die Teilneh-

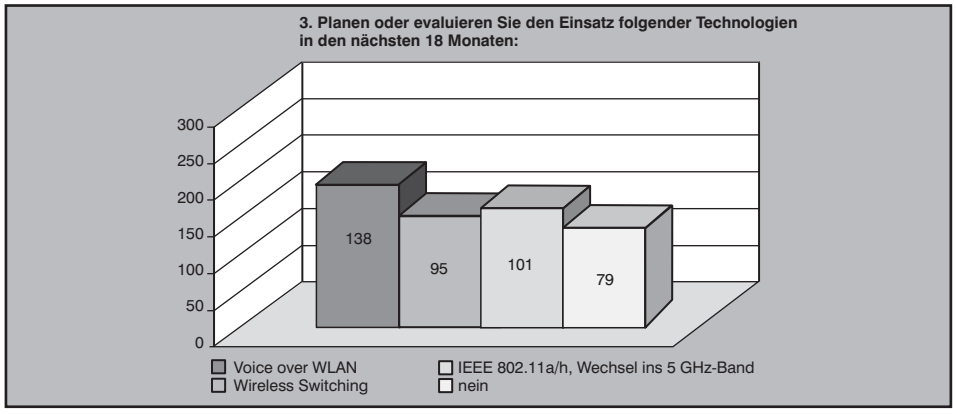


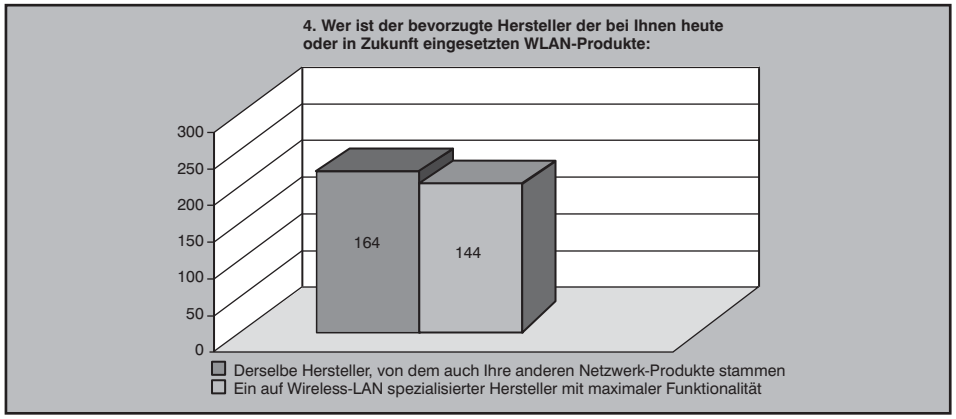


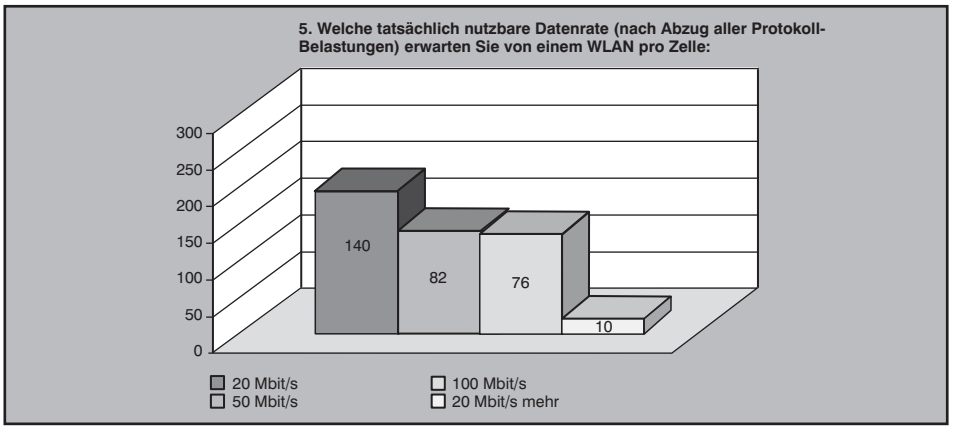


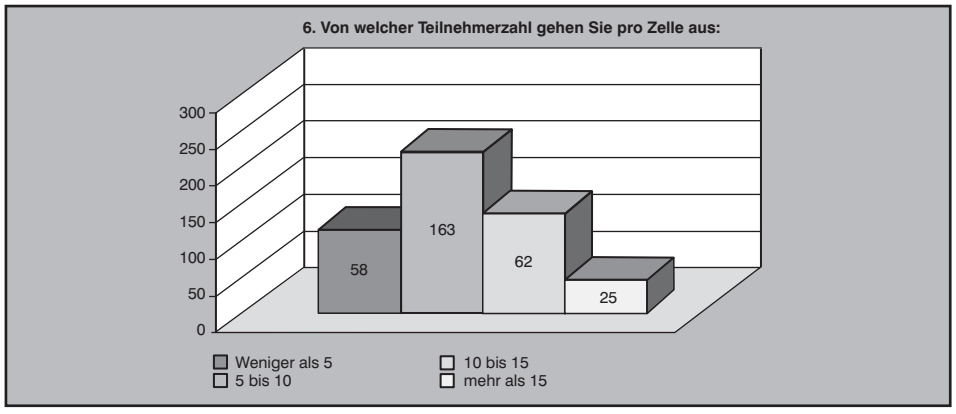


Wireless LAN Marktumfrage









mer der Umfrage eine Alternative, aber nicht der zwingende Weg. Ein genereller Wechsel auf Wireless-Switching ist in den nächsten 2 Jahren nicht zu erwarten. Allerdings wird diese Technologie stark an Bedeutung gewinnen. Überraschend ist, dass gleichzeitig der Roaming-Eigenschaft eine hohe Bedeutung zugemessen wird. Wireless-Switches sind eine denkbare Lösung für Layer-3-Roaming. Aus der Abweichung zwischen den Antworten zu diesen beiden Fragen kann ein gewisser Nachholbedarf in der Evaluierung von Wireless Switches abgeleitet werden.

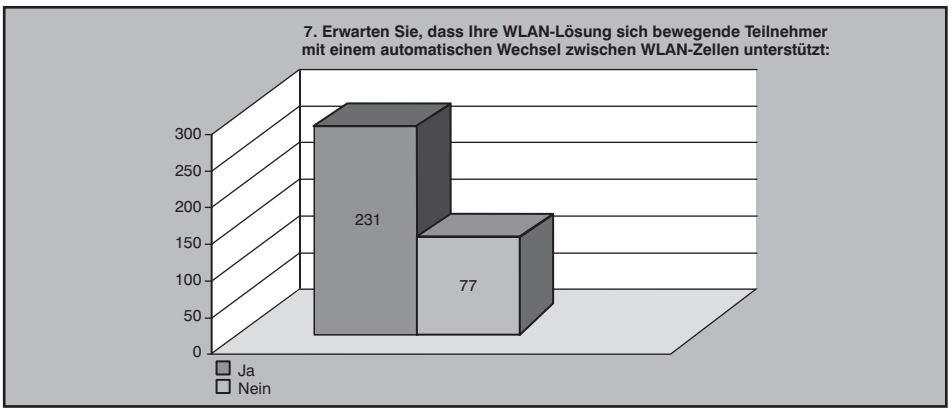
- Die Umfrage hat den Trend zu Voice over WLAN bestätigt. Technisch wird dies für die meisten Unternehmen noch Jahre dauern bis sie diesen Weg in der Masse gehen, wichtig ist hier, dass alle laufenden Planungen darauf ausgelegt werden, dass WLANs Voice-Ready sind. Hier ist es wichtig, dass die betroffenen Unternehmen erkennen, dass besondere Zellplanungen erforderlich sind und vor allem geeignete Handover-Lösungen gefunden werden müssen.

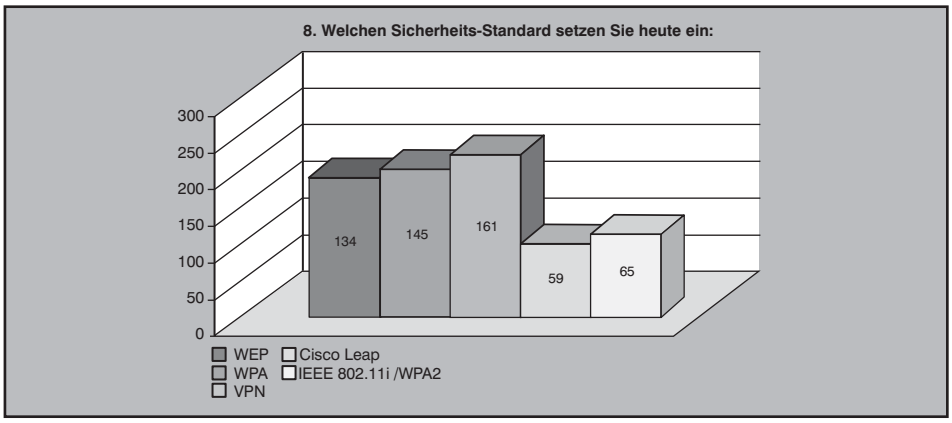
- Es herrscht offensichtlich Unklarheit über das Leistungsspektrum von Wireless-Switches, da sich die Antworten im Bereich Voice over WLAN und im Bereich Wireless Switching nicht decken. Voice over WLAN wird in den meisten Fällen Layer-3-Roaming erfordern.

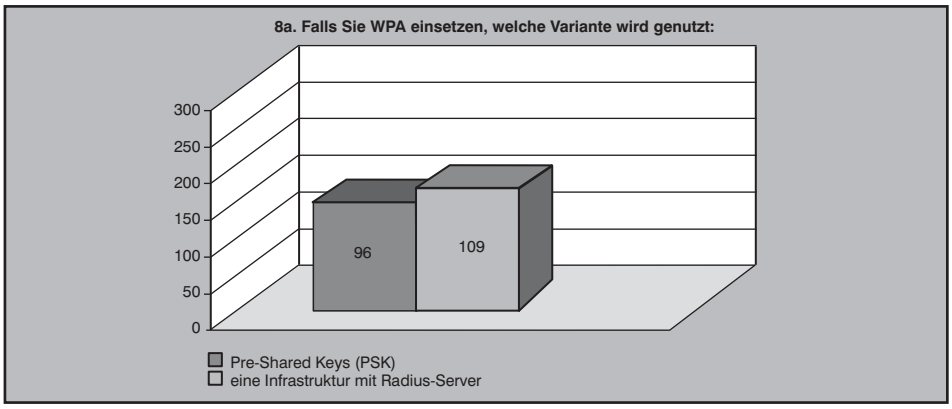
- Der Einstieg in das 5 GHz-Band hat begonnen. Nicht alle Hersteller unterstützen diesen Einstieg in geeigneter Form, doch ist die Auswahl an professionellen und zukunftsorientierten Produkten groß genug. Der Weg in flächendeckende Lösungen wird in vielen Fällen untrennbar mit dem Einstieg in die 5 GHz-Welt verbunden sein. Die hohe Zahl von b/g-Clients wird hier aber auf jeden Fall eine rückwärtskompatible Lösung erfordern. Dual-Radio-Access-Points sind hier das Maß der Dinge (Dual Radio meint hier zwei tatsächlich komplett gleichzeitig arbeitende Radioteile).

- Wireless LANs werden zur Standard-Technologie im Fertigungsbereich. Die Nachfrage hier ist hoch, auch unsere Umfrage bestätigt diesen Trend. Dabei darf nicht übersehen werden, dass Fertigungs-Umgebungen ganz eigene Anforderungen an Montage, Verfügbarkeit, Redundanz und Betriebssicherheit stellen. Auch das Thema Stabilität und saubere Zellenausleuchtung kann hier wesentlich komplexer sein. Für große Ausdehnungen wird man auf Dauer an

Wireless LAN Marktumfrage







den Vorteilen von 11a nicht vorbei kommen. Auch IEEE 802.11n hat durch die im Standard angestrebte stabilere Ausleuchtung das Potenzial zur Fertigungs-Technik (dies erfordert angesichts der sensiblen Umgehung aber auf jeden Fall weitgehende Kontrollmessungen)

- Bereits bei einem hohen Anteil der antwortenden Unternehmen werden die Sicherheits-Lösungen auf der Basis einer Radius-Infrastruktur realisiert. Es deutet sich an, dass dies zum Standard wird und dass PSK-Lösungen auf Dauer nicht Bestand haben werden. Eine Reihe der Umfrageteilnehmer arbeiten mit VPN-Lösungen. Diese können noch aus der Zeit stammen, in der es keine sinnvolle Alternative gab. Auch kann es sein, dass hier eine Ende-zu-Ende-Verschlüsselung gefordert wird. Mit höherer Teilnehmerzahl kann diese Lösung teuer werden oder nicht mehr skalieren

- Der relativ hohe Anteil an WEP-gesicherten WLAN-Installationen ist nicht wirklich überraschend, bieten doch immer noch eine Reihe von Clients keine andere Alternative. Wer Clients hat, die mehr können, der ist sicher gut beraten, einen Wechsel in eine andere Sicherheitstechnik zu vollziehen.

- 11n wird die meisten Anforderungen, die heute bestehen, erfüllen. Betrachtet man die Antworten im Bereich Datenrate und Teilnehmerzahl, dann deutet Alles darauf hin, dass gerade 11n eine hohe Investitionssicherheit und zum ersten Mal einen längeren Wireless-Lebenszyklus bieten wird. 11n scheint die Technik der Zukunft zu sein.

Weitergehende Antworten und Analysen zu den aufgeworfenen Fragen werden wir auf dem Wireless LAN Forum 2005 in Königswinter geben.

Top-Kongress

Wireless-LAN-Forum 2005

Die Comconsult Akademie veranstaltetvom 21. - 23. November das Wireless LAN Forum 2005.

Das Wireless LAN Forum 2005 ist unsere Top-Veranstaltung zu neuen Netzwerk-Technologien des Jahres 2005.

- Exklusiv-Analysen der technischen Entwicklung
- Der Markt und seine Zukunft in der Analyse
- Erfahrungs-Berichte aus aktuellen Projekten
- Praxis-orientierte Empfehlungen und Tipps

Wireless LANs haben sich mit einem jährlichen Umsatz von mehr als einer Milliarde US-Dollar bei weiterhin stark steigendem Trend zu einer Top-Technologie entwickelt. Sie stellen einen wesentlichen Teil unserer zukünftigen Netzwerk-Infrastruktur dar. Wichtige Anwendungen wie Telefonie, Produktionssteuerungen und Warenlogistik setzen eine WLAN-Infrastruktur voraus.

WLAN-Technik und WLAN-Produkte unterliegen einem starken Wandel. Zukunftssichere Investitionsentscheidungen erfordern eine genaue Kenntnis der aktuellen Entwicklungen

Folgende Trends dominieren:

- Neue WLAN-Technologien greifen die etablierten Backbone- und Campus-Netzwerke an und bieten mit einer vermaschten Architektur sowohl Stabilität als auch hohe Performance, Intel bezeichnet diese Entwicklung als: „the most important thing since the internet itself“

- Die traditionelle WLAN-Technik bestehend aus Client-Adapter und Access-Point wird immer mehr von der Konsumer-Technik bestimmt. Der Anfang 2006 zu erwartende neue IEEE 802.11n-Standard ist eindeutig auf den Konsumer-Markt ausgelegt. Auf der einen Seite werden Konsumer-Produkte dabei immer professioneller, auf der anderen Seite werden wichtige Anforderungen von Enterprise-Netzwerken nicht erfüllt

- Im Enterprise-Markt geht der Trend in Richtung Wireless-Switches und weg von den bisherigen einfachen Strukturen. Diese lösen viele WLAN-typische Probleme, sie sind vergleichbar mit dem Übergang von Repeatern auf Switches in der Kabel-gebundenen Infrastruktur. Sie haben aber durch ihre erhöhte Komplexität auch signifikante Nachteile, die man kennen muss. Die Entscheidung für das „richtige“ Produkt ist nicht einfach

- Für viele mittelständische Anwender mit kleineren WLAN-Infrastrukturen wird der Einsatz von High-End-Konsumer-Technik unter bestimmten Rahmenbedingungen eine Alternative sein. Dazu kann es notwendig sein, dass die Konsumer-Produkte um geeignete Verwaltungs- und Überwachungsprodukte ergänzt werden

- Nach der Verabschiedung von IEEE 802.11i sind WLANs nur noch mit einer begleitenden Sicherheits-Infrastruktur auf der Basis von IEEE 802.1X und eines Radius-Servers akzeptabel

- Die zunehmenden massiven Probleme in den USA mit dem 2,4 GHz-Frequenzband führen zu einem starken Wechseltrend ins 5 GHz-Band, selbst im Konsumer-Bereich sind die Interferenz-Störungen inzwischen so massiv, dass Panasonic seine traditionellen Funktelefone in den 5 GHz-Bereich verlagert (nicht in die WLAN-Frequenzen)

Das Wireless LAN Forum 2005 greift diese Entwicklungen auf, informiert über die Trends hinter den Kulissen aus der Normung und den Hersteller-Labors. Wichtige Entwicklungen werden von ComConsult Research exklusiv für dieses Forum analysiert.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Wireless-LAN-Forum 2005

☐ Ich buche den Kongress
Wireless-LAN-Forum 2005
vom 21.11. - 23.11.05 in Königswinter
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht: Wireless LAN Forum 2005

Montag, den 21.11.2005

9:30 - 10:45 Uhr und 11:15 - 12:30 Uhr

Neue WLAN-Technologien in der Analyse: wohin wird die weitere Entwicklung gehen

- IEEE 802.11: aktuelle Entwicklungen und die Zukunft
  - Kampf um IEEE 802.1n: Konsumer kontra Enterprise, wer gewinnt?
  - IEEE 802.11n: der neue Standard in der Analyse
  - Wie arbeitet er
  - Können die bisherigen Schwachstellen beseitigt werden
  - Reichweite, Datenraten, Stabilität
  - Was kommt nach 11n: Ausblick auf zukünftige Wireless-Potenziale
- Was machen die Chip-Hersteller
  - Atheros und der Einfluss auf die Access-Point-Technologie
  - Airgo und die Bedeutung neuer Standards, oder: wer außer Airgo kann 802.11n rechtzeitig liefern
  - Broadcom: vom Wireless-Client zur Switch-Integration, in welchem Umfang wird Wireless-Switching in Zukunft eine Standard-Eigenschaft von Switch-Systemen sein
  - Intel: der Client bestimmt die WLAN-Technologie, welchen Einfluss kann Intel auf die zukünftige Wireless-Entwicklung durch seine starke Position im Notebook-Markt nehmen?
- IEEE 802.15 und IEEE 802.16: die Wireless-Revolution
  - Technische Hintergründe
  - Schlüsselfrage Client-Integration
  - Zusammenspiel mit 802.11: Aufbau einer Wireless-Hierarchie
  - Zeitachse und Ausblick
- Fazit: Empfehlungen für zukünftige Investitionen auf der Basis der beschriebenen Entwicklungen

Dr. F.-J. Kauffels, Unternehmensberater

14:00 - 15:30 Uhr

Netzwerk-Design 2005 und Integration von Wireless-LANs

- Bewertungskriterien für ein bestehendes Netzwerk-Design
- Neue Ansätze im Campus-Design
- Neue Verfahren im Tertiär-Bereich zur Optimierung von Konvergenz-Zeiten
- Integrations-Alternativen für WLAN-Netzwerke
  - Einzel-Zellen
  - Mehrzellen-Installationen
  - Sonderfall Wireless-Switches
- Die Rolle des Sicherheits-Konzepts
- Voice-ready und Quality-of-Service: was ändert sich durch WLANs?
- Integrierte Redundanz-Lösungen für Kabel-LAN und WLAN
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Resultierende Design-Alternativen und ihre Nutzbarkeit
- Beispiele

Dipl.-Inform. Petra Borowka, UBN

16:00 - 17:30 Uhr

Switch-basierte WLAN-Architekturen kontra traditionelle Lösungen: wohin geht der Markt und wie verändert sich WLAN-Design?

- Konzepte der Hersteller (Cisco, Trapeze, Chantry, Aruba) im Vergleich
- Wie arbeiten die verschiedenen Lösungen, was leisten sie?
- Kommt der universelle Access-Point, der sich nur noch in der Software unterscheidet?
- Welches Control-und Provisioning-Protokoll für APs wird sich durchsetzen?
- Die IETF-CAPWAP-Norm: Architekturen und Protokolle
- Leightweight Access Point Protocol LWAPP vs. CAPWAP Tunneling Protocol
- Wo stehen andere Ansätze wie SLAPP, was wird Chantry machen?
- Wie offen werden diese Lösungen wirklich sein?
- Integration im Switch: wird Wireless-Switching in Zukunft ein Standard-Element jedes normalen Switches sein?
- Layer-3-Roaming, Trouble Shooting, Redundanzkonzepte
- Das virtuelle Distribution System als Standard-WLAN-Design
- Management von WLANs aus der Perspektive von Wireless-Switches
- Empfehlungen aus laufenden Projekten

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 22.11.2005 - vormittag

9:00 - 9:45 Uhr

Der Wechsel ins 5 GHz-Band: erfordern Interferenzen den Wechsel ins 5 GHz-Band für einen sicheren und stabilen Betrieb und wie werden 11b-Geräte integriert

- Gefahren im 2,4 GHz-Band
- Betriebs-Herausforderung: Erkennung von Interferenz-Problemen
- Merkmale einer 5 GHz-Lösung
- Ausleuchtung, Stabilität und Planung in der Analyse
- 11a kontra 11h: was 11h wirklich leistet, WiFi-Zertifizierung
- DFS und TPC und die Konsequenzen
- Sendeleistungen und Kanalwahl
- Reichweiten in Abhängigkeit von der Sendeleistung
- 5 GHz als Outdoor-Bridging: Nutzung der hohen Sendeleistungen
- Einbindung von 11b und 11g
- Multi-Radio-Acess-Points: ist dies der Trend? Sind Investitionen in Dual-Band/ Single Radio eine Fehlinvestition?
- Werden 5 GHz-Lösungen durch ihre hohe Kanalzahl zu Array-Lösungen tendieren? Sind Array-Lösungen eine echte Alternative?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr

Voice over WLAN: wie Sie ihre WLAN-Lösung Voice-tauglich machen

- Warum Sie von der Existenz von Voice over WLAN in Ihrem Netz ausgehen müssen
- Eignung von WLANs für Telefonie-Anwendungen
- IEEE 802.11e und WiFi-Multimedia: Technik und Produkte
- Sinn und Grenzen von Quality of Service, Integration mit dem Kabel-LAN
- Verschärfte Anforderungen an die Zellplanung: was ist anders als im Sprach-losen WLAN
- Was Endgeräte leisten müssen
- Wie offen kann eine Lösung sein?
- Integration in die Kabel-basierte VoIP-Landschaft
- Absicherung der Sprachübertragung: was heute schon möglich ist und worauf noch gewartet werden muss

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

11:00 - 11:45 Uhr

WLANs in der Fertigung
Wireles LANs in der Produktion

- WLAN-Eignung für das Produkstionsumfeld
- Anforderungen an Access Points
- Montage in rauen Umgebungen
- Mobile Anwendungen in der Fertigung: schneller Zellwechsel und Alternativen in der Umsetzung
- Echtzeit und WLAN: wie ist das zu bewerten, wo liegen die Grenzen
- Interferenzen: wo ist damit zu rechnen, was ist zu tun
- Funk-Ausleuchtung von Industrieumgebungen: was man wissen muss
- WLAN-Verfügbarkeit und seine Grenzen
- Neue Funktionen und Einsatzgebiete mit Siemens-Produkten
- Anwendungsbeispiel, Empfehlungen

Nicolas Heise, Siemens AG

11:45 - 12:30 Uhr

Ausbau der Wireless-Technologie, wohin geht Cisco, wie sieht die Migration aus?

- Airespace und Aironet: wohin geht der Weg?
- Wie sehen zukünftige Architekturen nach Anwendungsfeldern aufgeteilt aus:
  - Notebook-Integration an ausgewählten Flächen
  - Flächendeckend, nicht mobil (handover keine Forderung) - mobil
- Integration vorhandener Produkte: was wird aus Aironet?
- Wohin geht der Weg bei Neuprodukten?
- Welchen Stellenwert werden AccessPoints mit Multi-Radio haben?
- Wie viele Radios werden kommen? Wird Cisco auch Arrays einsetzen?
- Mit welcher Sendeleistung in welchen Frequenzen wird Cisco bei 11a/h in Zukunft arbeiten?
- Was wird aus WLSM und dem vorhandenen 6500 Blade
- LWAPP und was es leistet
- Wie offen ist LWAPP, wird die Cisco-Implementierung dem RFC entsprechen?
- Was macht Cisco, wenn die CAPWAP-Normung andere Protokolle unterstützt?
- Wired-Switching und Wireless-Switching: wachsen die Welten zusammen?
- Was heißt das konkret für Cisco: kommt ein neues Blade für den 6500?
- Wird eine Implementierung auch in andere Switch-Familien erfolgen?
- Wird das für vorhandene Switches nachrüstbar sein?
- Wireless-Switching und die Integration von APs anderer Hersteller
- Location Server
  - Was leistet der Location Server?
  - Wie funktioniert die Standort-Ermittlung?
  - Wie sehen sinnvolle Anwendungs-Szenarien in Europa aus?
  - Ist es geplant, Standort-Informationen in Lastverteilungs-Algorithmen zu integrieren?
- Voice over wireless
  - Wo steht Cisco?
  - Wie sieht die Unterstützung von Clients von Drittherstellern aus?

Bernd Hillemeister, Cisco Systems

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause

Programmübersicht: Wireless LAN Forum 2005

Dienstag, den 22.11.2005 - nachmittag

14:00 - 14:45 Uhr
Wireless Switching und Voice over WLAN: untrennbar verbunden?
- Architektur und technische Schwerpunkte
- Migrationswege von Fat-APs zu Wireless Switches
- Voice over WLAN: was leistet Siemens?
- Gibt es Besonderheiten für HiPath-Lösungen?
- CAPWAP: wo steht Siemens?
- Offenheit der Lösung
- Wie können Access-Points anderer Hersteller integriert werden?
- Integration von Voice-Anwendungen von Drittherstellern
- Was ist mit 11a/h und Multi-Radio-Lösungen
- Wie sieht die Zukunft aus: was ist mit 11n und WiMAX?

Dirk Abel, Siemens AG

14:45 - 15:30 Uhr
Wireless Switching und Layer-3-Roaming
- Architektur und technische Schwerpunkte
- Was leistet das Planungs-Tool?
- Roaming bei Trapeze
- CAPWAP: wo steht Trapeze?
- Offenheit der Lösung
- Integration der Access Points von Drittherstellern
- Was bedeutet die Zusammenarbeit mit Nortel und Enterasys für den Markt?
- Was ist mit 11a/h und Multi-Radio-Lösungen?
- Wie sieht die Zukunft aus: was ist mit 11n und WiMAX?

Reinhard Müller, Trapeze Networks

16:00 - 16:40 Uhr
Neue Technologien bei Wireless-Switches
- Data Plane kontra Control Plane: Wo liegen die Unterschiede, wo liegen die Vorteile für den Anwender?
- Ist eine stufenweise Migration von Fat APs zu Wireless-Switching denkbar? Wie können Investionen in traditionelle Wireless-Technik abgesichert werden?
- Integration von Wireless-Lösungen in eine umfassende Sicherheits-Konzeption
- Wann kommt 11n? Wie wird es integriert?

Dipl.-Ing. Markus Nispel, Enterasys Networks

16:40 - 17:15 Uhr
Podiumsdiskussion
- Verdrängen Wireless-Switches traditionelle Ansätze im Enterprise-Markt?
- Lohnen sich große Investitionen noch vor der Verfügbarkeit von 11n?
- Wie offen werden diese Lösungen sein?
- Ist CAPWAP ein toter Standard oder wird sich wirklich jemand daran halten?
- Sind Prosumer-Produkte eine Alternative?
- Ist das 2,4 GHz-Frequenzband tot, liegt die Zukunft bei 5 GHz?
- Sind Access-Points mit nur einem Radio (Dual-Band, Single Radio) eine Fehlinvestition?
- Wird Voice over WLAN die Zukunft prägen?
- Ist WLAN-Sicherheit ohne Sicherheits-Infrastruktur erreichbar?

15:30 - 16:00 Uhr Kaffeepause

Mittwoch, den 23.11.2005

9:00 - 10:15 Uhr
WLAN-Planung und Betrieb 2005: Planungs- und Betriebsansätze für eine sichere, stabile und performante WLAN-Zukunft
- Was leisten Tools für Site-Survey und Netzplanung?
- Access-Punkt basiertes Site Survey
- Monitoring der Luftschnittstelle: Fehlersituationen, Performance-Indikatoren, Messtechnik und ihre Auswirkung auf Planung und Betrieb
- Automatische Kanalzuweisung
- Dynamische Einstellung der Sendeleistung
- Last-Verteilung zwischen den Access-Points
- Management von Mobilität, Roaming und Handover
- Erkennung und Bewertung von Interferenzen im laufenden Betrieb
- Einfluss der herstellerspezifischen Lösungsansätze
- Empfehlungen aus der Praxis

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
Fast Roaming: Wireless-Infrastrukturen für mobile Teilnehmer
- Ausgangslage: Roaming-Problematik
- Konkrete Benennung messbarer Anforderungen
- Lösungsansätze im Standard
- Lösungsansätze der Hersteller
- Sicherheit und Mobilität
- Pre-Athentication nach 802.11i
- Zentrale Verwaltung der Schlüssel-Informationen
- Roaming-Vorteile der Wireless-Switch-Technik

Dr. - Ing. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:30 - 12:30 Uhr
Anwender-/Projektbericht: Der Siemens-Konzernstandard für Wireless-LANs
- Warum Wireless-Netzwerke einen Konzernstandard erfordern
- Ausgangslage im Siemens-Konzern
- Inhalt des Konzernstandards
- Besondere Anforderungen von Produktions-Standorten
- Besondere Anforderungen von Büro-Umgebungen
- Welche Teile waren kontrovers?
- Erfahrungen in ersten Pilotprojekten
- Empfehlungen und Erfahrungen aus dem bisherigen Projektverlauf

Dipl.-Ing. Bernhard Rößler, Siemens AG

14:00 - 15:00 Uhr
WLAN-Sicherheit praxisgerecht umsetzen
- WPA, WPA2 und IEEE 802.11i
- IEEE 802.11X: Gestaltungsalternativen im Vergleich
- Infrastruktur kontra Pre-Shared-Key: warum die Infrastruktur notwendig ist
- Geräte-oder Nutzer-Identifizierung?
- Was zum Aufbau der Infrastruktur zu machen ist
- Wo denkbare Probleme liegen
- Wie Teilnehmer und deren Geräte klassifiziert und in Benutzergruppen mit separaten Rechten eingeteilt werden können
- Integration von Gästen: Risikobetrachtung und Bewertung der verfügbaren Techniken
- Integration in eine Gesamtlösung für WLAN und Kabel-LAN

Markus Schaub, ComConsult Technologie Information GmbH

15:00 - 15:45 Uhr
Neue Wireless-Technologien und Elektrosmog
- Ausgangslage
- Physikalische und dosimetrische Quantifizierung
- Neue Empfehlungen des NRPB
- Beurteilung der EU-Kommission
- Die Ergebnisse des REFLEX-Projektes
- Konsequenzen für bestehende Grenzwerte, z.B. CE-Zertifizierung
- Gesenkte Grenzwerte und ihr Verhältnis zu aktuellen WLAN-Technologien
- Verantwortungsvolle vorsorgeorientierte Planung
- Erweiterte Möglichkeiten mit neuen Technologien

Dr. F.-J. Kauffels, Unternehmensberater

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Report des Monats

Neuerscheinung
Wide Area Networks - Leistungsfähige WAN-Strukturen für zentrale Dienste

Lesen Sie im Folgenden einen Ausschnitt aus der Studie „Wide Area Networks - Leistungsfähige WAN-Strukutren für zentrale Dienste“.

1.1 Grundlegende Unterschiede zu LAN
Trotz verbesserter Leistungsparameter von WAN gelten in Weitverkehrsnetzen nach wie vor besondere Rahmenbedingungen, die mit Verhältnissen wie sie in modernen lokalen Netzen vorherrschen nicht vergleichbar sind. Zu diesen Besonderheiten, die bei der Planung des Applikationseinsatzes in WAN-basierten Szenarien auf jeden Fall berücksichtigt werden müssen, gehören u.a. folgende Aspekte:

- Die Bandbreite, die den Applikationen zur Verfügung steht, ist - bedingt durch die im Vergleich zu LANs erheblich höheren Kosten - typischerweise geringer als im LAN.
- Die Anzahl der Hops zwischen Client und Server ist bedingt durch die Netzinfrastruktur in der Regel vergleichsweise hoch.
- Der Packet Delay ist aufgrund der mit der höheren Netzauslastung verbundenen, längeren Verweildauer in den Sende-Queues, vor allem aber wegen der geografischen Distanz deutlich höher als in LANs.
- In großen Netzen ist die Netzstruktur nur selten homogen.
- Eine durchgehende Bereitstellung von QoS ist in vielen Fällen schwierig.

Vor diesem Hintergrund ist festzuhalten, dass bei weitem nicht jede Applikation WAN-tauglich ist. Im Gegenteil: da praktisch alle Client-Server-Anwendungen - von Ausnahmen wie Web-basierenden Anwendungen und Terminal-Server-Systemen einmal abgesehen - im LAN-Umfeld entwickelt, getestet und zumindest bisher meist auch eingesetzt wurden, sind Probleme beim Versuch, eine solche Applikation in ein WAN-dominiertes Szenario zu portieren, praktisch vorprogrammiert. Applikationsverhaltensweisen, die im LAN

tolerierbar sind, sind dies im WAN nicht automatisch, so dass „empfindliche“ Applikationen, d. h. solche, deren Mechanismen sich allzu sehr auf LAN-Bedingungen stützen, hier schnell Probleme verursachen können.

Natürlich lassen sich viele WAN-typische Nachteile durch vermehrten Ressourceneinsatz umgehen, allerdings geht dies zu Lasten der Wirtschaftlichkeit, und längst nicht jedes technische Problem lässt sich auf diesem Wege ausräumen.

Ein Grundproblem des Applikationseinsatzes im WAN ist die dabei angewandte Strategie, die vorsieht, bei der Portierung einer LAN-Applikation auf ein WAN-Szenario - der „Klassiker“ ist hier die Zentralisierung bislang dezentraler Applikationsserver - das WAN an die Erfordernisse der Applikation anzupassen. De facto bedeutet das, durch ein entsprechendes Netzdesign auch in der WAN-Umgebung vergleichbare Leistungsparameter wie im LAN sicherzustellen.

Die Folgen dieses Ansatzes sind nicht unerhebliche Kosten für die erforderliche Bandbreite und eventuell notwendige Mechanismen für die Realisierung von QoS (Quality of Service). Beim Blick auf das Budget für eine solche Migration stellt man in der Regel fest, dass dieses für die im WAN notwendigen Maßnahmen nicht ausreicht, weil die Kosten für eine Umsetzung der Anforderungen an das WAN fast immer mehr oder minder deutlich unterschätzt werden. Es muss also meist ein gewisser Mangel verwaltet werden. Dies lässt sich mittels intelligenter Mechanismen der Verkehrssteuerung in gewissen Grenzen realisieren, allerdings mit nicht unbeträchtlichem Aufwand. Außerdem darf keinesfalls vergessen werden, dass auch solche Verkehrssteuerungssysteme die physikalischen Grenzen des WAN nicht außer Kraft setzen: ist beispielsweise der Ende-zu-Ende-Delay zu hoch, nutzt der beste und intelligenteste Mechanismus zur Bandbreitenzuteilung nichts.

Die bessere Alternative liegt daher in einer gezielten Auslegung betroffener Applikationen für den Einsatz unter WAN-Bedingungen. Wo eine entsprechende gezielte Anpassung, beispielsweise durch Vergrößern der Delay-Toleranz, nicht möglich ist - dies dürfte vor allem bei kommerziellen (Standard-)Applikationen der Fall sein - sollten diese auf WAN-Tauglichkeit geprüft und gezielt danach ausgewählt werden. Eigenentwicklungen sollten auf jeden Fall

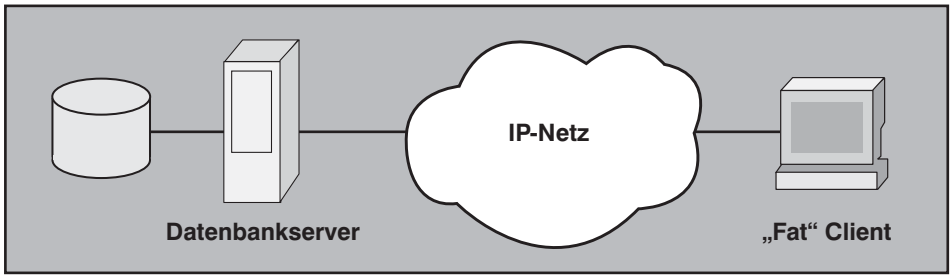


Abbildung 1: Direkter Client-Zugriff auf den Datenbankserver

Source	Destination	Bytes	Rel. Time	Delta Time
[Client]	[Server]	413	0:00:00:000	24
[Server]	[Client]	105	0:00:00:000	413
[Client]	[Server]	117	0:00:00:000	175
[Server]	[Client]	165	0:00:00:001	520
[Client]	[Server]	145	0:00:00:001	105
[Server]	[Client]	105	0:00:00:001	256
[Client]	[Server]	117	0:00:00:001	86
[Server]	[Client]	140	0:00:00:001	255
[Client]	[Server]	382	0:00:00:002	351
[Server]	[Client]	105	0:00:00:002	373
[Client]	[Server]	117	0:00:00:002	96
[Server]	[Client]	565	0:00:00:003	922
[Client]	[Server]	172	0:00:00:003	265
[Server]	[Client]	105	0:00:00:004	272
[Client]	[Server]	117	0:00:00:004	95
[Server]	[Client]	152	0:00:00:004	261
[Client]	[Server]	145	0:00:00:004	74
[Server]	[Client]	105	0:00:00:004	250
[Client]	[Server]	117	0:00:00:004	86
[Server]	[Client]	140	0:00:00:005	255

Tabelle 1: Paket-Trace für das Fat-Client-Szenario

entsprechenden Anpassungen unterworfen werden, welche die Rahmenbedingungen des WAN berücksichtigen.

1.2 Exemplarischer Vergleich von Anwendungen

In diesem Abschnitt werden Anwendungen mit unterschiedlichen Architekturen und Kommunikationsprofilen einem exemplarischen Vergleich unterzogen. Diese Gegenüberstellung soll die Auswirkungen ungünstiger Verkehrsprofile auf Antwortzeiten im WAN veranschaulichen und dazu motivieren, der Anpassung von Applikationen an die Belange von WAN die gebührende Bedeutung beizumessen.

1.2.1 Datenbankzugriffe über das WAN

Viele Benutzer von Datenbankapplikationen haben die Erfahrung gemacht, dass solche Applikationen zwar im LAN, jedoch nicht im WAN mit akzeptablen Antwortzeiten funktionieren. Dabei ist weniger die Bitrate des WANs, sondern die durch lange Entfernungen verursachte Signallaufzeit das Problem. Die nachfolgend beschriebenen Untersuchungen belegen diese Aussage.

Zum Vergleich verschiedener Anwendungsarchitekturen für Datenbanken wurde in Tests die gleiche Applikation mit drei verschiedenen Architekturen untersucht, auf die im Folgenden eingegangen wird.

1.2.1.1 Direkter Clientzugriff auf den Datenbankserver

Der erste Fall ist in Abb. 1 dargestellt.

Beim Datenbankserver handelte es sich um einen Server mit einer SQL-Datenbank, beim Client um einen vollwertigen Datenbankclient („Fat Client“). Mit diesem Client wurde auf dem Datenbankserver eine bestimmte Folge von Zugriffen auf Datensätze durchgeführt und mittels eines auf dem Client laufenden Analyseprogramms (Ethereal) protokolliert.

Die nähere Analyse des Lastprofils von Datenbankapplikationen mit Fat Clients durch ComConsult hat ergeben, dass bei Nutzung von Protokollen wie Transparent Network Substrate (TNS) bzw. SQL.net zu den wichtigsten Merkmalen des Lastprofils der Umstand gehört, dass der Server auf ein Paket des Clients mit einem Paket reagiert und umgekehrt. D. h. ein „Bursting“ in dem Sinne, dass der Server eine Anfrage mit der Übermittlung einer ununterbrochenen Folge von Paketen beantwortet, findet nicht statt. Server und Client wechseln sich als Sender bzw. Empfän-

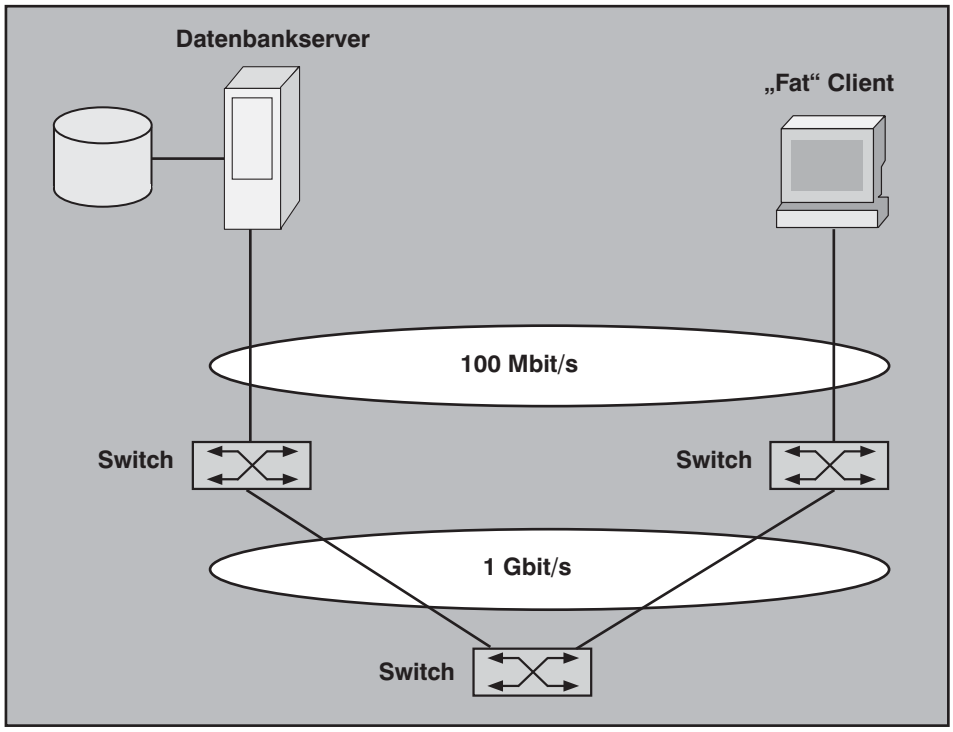


Abbildung 2: LAN-Szenario

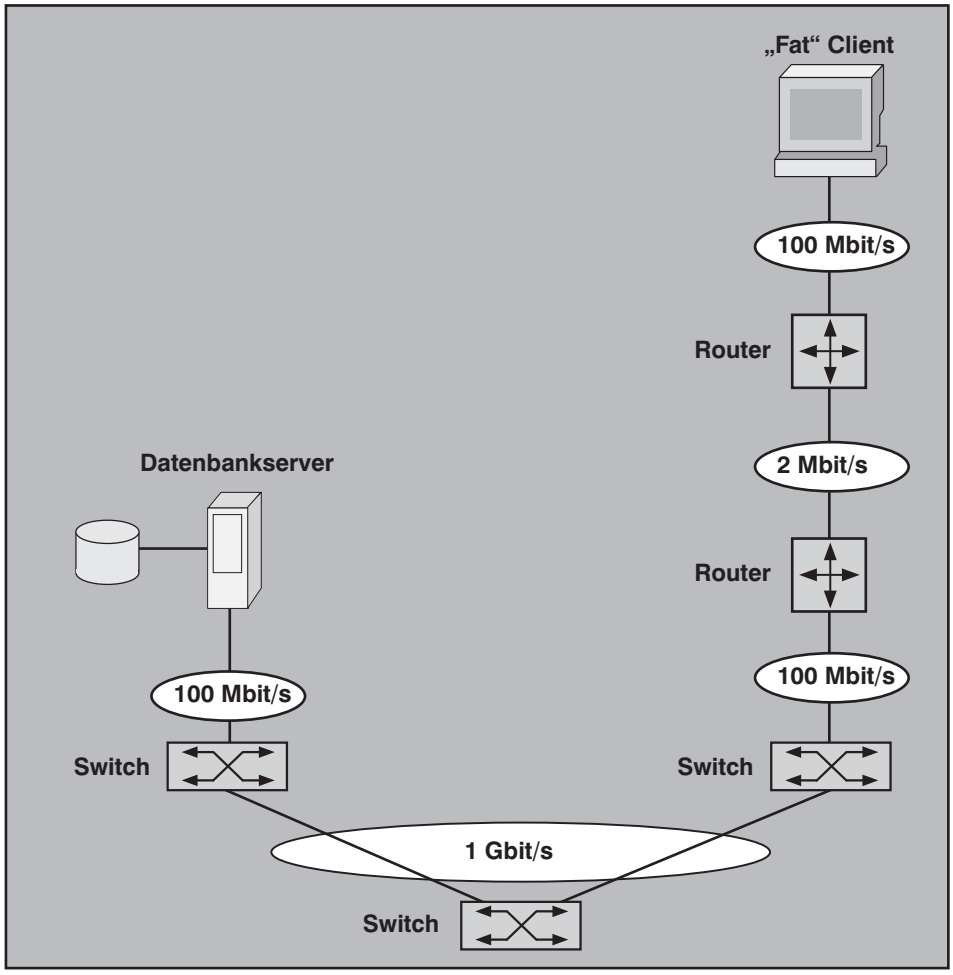


Abbildung 3: WAN-Szenario

ger ständig ab. Für jedes Paketpaar ist als Übertragungszeit die volle Round Trip Time (RTT) zwischen Client und Server zu berücksichtigen. Werden so z. B. 4.000 Pakete vom Server zum Client und vom Client zum Server übertragen, entsteht eine Gesamtlatenz von 4.000*RTT bzw. 8.000*OneWayDelay.

Ein solches Kommunikationsprofil ist dann besonders problematisch, wenn der Delay im Netz (Signalverzögerung) steigt.

Tabelle 1 zeigt anhand des Auszugs aus dem aufgezeichneten Paket-Trace das typische Kommunikationsprofil eines Fat-Client-Szenarios.

Jede Zeile stellt ein Paket dar. In der ersten Spalte ist die Quelle, in der zweiten das Ziel angegeben. Die dritte Spalte gibt die Paketlänge in Bytes wieder, die vierte Spalte den Zeitstempel im Format h:mm:ss.Millisekunde. Die Einheiten für die Werte in der fünften Spalte, die den Abstand jedes Paket zum vorangegangenen Paket wiedergibt, sind Mikrosekunden.

Die Messung wurde in einem LAN mit 100 Mbit/s vom Client zum ersten Switch, 1 Gbit/s vom ersten zum zweiten und vom zweiten zum dritten Switch sowie 100 Mbit/s vom dritten Switch bis zum Server durchgeführt (siehe Abbildung 2).

Der gesamte Ablauf mit den bestimmten Arbeitsschritten dauerte ca. 25 Sekunden und war mit der Übertragung von ca. 250 KBytes verbunden.

Nun stelle man sich vor, zwischen Client und Server liege eine direkte WAN-Verbindung mit der Übertragungsrate 2 Mbit/s wie in Abbildung 3 dargestellt.

Das Hinzufügen einer WAN-Strecke zum LAN-Szenario wirkt sich wie folgt auf das Antwortzeitverhalten der Datenbankanwendung aus:

- Die Paketbildung für eine 2-Mbit-Strecke wirkt sich insofern aus, dass zur Gesamtantwortzeit die Zeit hinzugerechnet werden muss, die für die Übertragung von ca. 256 KBytes über die WAN-Strecke erforderlich ist. Diese Zeit beträgt ca. eine Sekunde.

- Gravierender wirken sich die Paket-Delays im WAN aus. Wie aus dem Paket-Trace hervorgeht, besteht das Kommunikationsprofil darin, dass in der Regel auf ein Paket des Clients ein Paket des Senders folgt. Jedes der Pakete muss die WAN-Strecke zurücklegen, bevor es das Ziel erreicht und von

diesem beantwortet wird. Die Anzahl dieser Zyklen, multipliziert mit dem Round-Trip-Delay (RTD) des WAN, ergibt die zusätzliche Verzögerung des gesamten Vorgangs durch den WAN-Delay. Oder anders gerechnet: Jedes Mal, wenn die Paketfolge die Richtung wechselt, ist ein One-Way-Delay des WAN als zusätzliche Verzögerung zu berücksichtigen.

Für das oben skizzierte Szenario und verschiedene WAN-Delaywerte wurde bei einer WAN-Bitrate von 2 Mbit/s die Gesamtdauer des Vorgangs in Tabelle 2 berechnet.

Während die Dauer der Paketbildung für die 2 Mbit/s mit 1,025536 Sekunden nicht bemerkbar ist, bedeutet bereits ein WAN-One-Way-Delay von 5 Millisekunden (entsprechend einem Kabelweg von ungefähr 1.000 km) eine Antwortzeitverschlechterung von 30 % im Vergleich zum LAN-Szenario. Geht man von einem globalen Szenario und einem WAN-Delay von 100 Millisekunden aus (theoretischer Mindestwert bei der Überbrückung einer Strecke ungefähr zwischen Deutschland und Neuseeland), würde die Antwortzeit sich auf mehr als das Sechsfache der Antwortzeit im LAN verschlechtern.

Als Zwischenfazit ist festzuhalten, dass ein direkter Zugriff eines Datenbank-Clients auf eine Datenbank über typische Datenbankprotokolle wie SQL.net nicht WAN-tauglich ist. Selbst wenn man im WAN die gleiche Bandbreite wie im LAN nutzen könnte, würde sich die wesentlich längere Signalausbreitungszeit zusammen mit dem ungünstigen Kommunikationsprofil des Fat-Client-Szenarios so auswirken, dass im Vergleich zum LAN im WAN wesentlich längere bis inakzeptable Antwortzeiten zustande kämen.

übertragende Bytes		256.384
Dauer für die Paketierung an der 2-Mb/s-Strecke		1.025.536 µs
Gesamtduaer der Übertragung im LAN		25.274.335 µs
WAN-Zyklen		1.312
Delay (one way) in µs	**Dauer des Vorgangs**	**Veränderung im Vergleich zum LAN-Szenario**
5.000	32.859.871	30 %
10.000	39.419.871	56 %
15.000	45.979.871	82 %
20.000	52.539.871	108 %
25.000	59.099.871	134 %
30.000	65.659.871	160 %
35.000	72.219.871	186 %
40.000	78.779.871	212 %
45.000	85.339.871	238 %
50.000	91.899.871	264 %
55.000	98.459.871	290 %
60.000	105.019.871	316 %
65.000	111.579.871	341 %
70.000	118.139.871	367 %
75.000	124.699.871	393 %
80.000	131.259.871	419 %
85.000	137.819.871	445 %
90.000	144.379.871	471 %
95.000	150.939.871	497 %
100.000	157.499.871	523 %

Tabelle 2: Auswirkung von WAN-Delay auf das Antwortzeitverhalten

ComConsult Research startet Initiative: Sichere und sensible Browser-Nutzung

Kostenfreie Vortragsunterlagen zur Ausbildung und Sensibilisierung von Endanwendern für Käufer eines Reports oder Teilnehmer an unseren Kongressen

Internet-Browser sind eine weiterhin zunehmende Quelle für Gefahren im Internet. Sie werden als Einfallstor für die verschiedensten Arten von Angriffen benutzt:

- Übernahme des PCs und Ausführung von Angriffen auf Dritte
- Ausspionieren von Passworten und anderen persönlichen Schutzrechten
- Verteilung von Viren und Trojanern

Leider lassen sich Browser nicht so konfigurieren, dass sie bei voller Funktionalität 100%ig sicher sind. Jede Erhöhung der Sicherheit geht speziell beim Internet Explorer einher mit der Einschränkung an Funktionalität.

Der Schlüssel zum sicheren Browser-Einsatz ist deshalb aus unserer Sicht nicht allein in der Konfiguration zu suchen. Im Vordergrund sollte die Sensibilisierung des Benutzers stehen. Der typische Benutzer muss ein Gefühl dafür entwickeln, wie riskant die Nutzung eines Internet-Browsers sein kann.

Um diese Sensibilisierung zu unterstützen hat ComConsult-Research die Initiative „Sichere und sensible Browser-Nutzung“ gestartet. Im Mittelpunkt der Initiative stehen Vortragsunterlagen zur Information und Sensibilisierung von Endanwendern.

Ab sofort erhält jeder Käufer eines Reports und jeder Besucher eines Kongresses diese Vortragsunterlagen zur kostenfreien Nutzung im eigenen Unternehmen.

Die Unterlagen dürfen zu diesem Zweck sowohl vervielfältigt als auch als Vortrag eingesetzt werden. Lediglich die Weitergabe an Dritte und jede Form der kommerziellen Nutzung wird ausgeschlossen.

Der Vortrag ist als lebender Vortrag konzipiert. Wir sind an Rückmeldungen und Verbesserungsvorschlägen sehr interessiert und werden diese nach Prüfung in die aktuelle Distribution einbauen.

Die aktuelle Version wurde zudem zum Einsatz an weiterführenden Schulen konzipiert, um die Schüler der Sekundarstufe 1 und 2 zu einem sensibleren Umgang mit dem Internet zu motivieren. Die Vortragsunterlagen sind generell für Schulen frei verfügbar.

Bitte wenden Sie sich an:
drsuppan@comconsult-research.com mit der Nennung der betroffenen Schule und des Ansprechpartners in der Schule, um die kostenfreie Schulversion zu erhalten.

Natürlich können Sie den Vortrag inkl. Referenten buchen und somit ein komplettes Paket zur Ausbildung Ihrer Endanwender erwerben.

Dieses Paket kann mit einem Zusatzvortrag über Browser-Management und insbesondere die unterschiedliche Handhabung des Internet Explorers im direkten Vergleich mit Firefox (1.07 und 1.5 Beta) ergänzt werden.

Bitte wenden Sie sich direkt an Herrn Cornelius Höchel-Winter choechel@comconsult-research.com, um die Details zu diesem Paket zu besprechen.

Können Sie die Vortragsunterlagen zur internen Nutzung auch erwerben, wenn Sie weder einen Report kaufen noch an einem Kongress teilnehmen? (Beides würden wir natürlich sehr bedauern).

Ja, die Möglichkeit des Kaufs der Unterlagen besteht.

Sie können die Vortragsunterlagen inkl. der beschriebenen Nutzungsrechte für 398,-- Euro zzgl. MwSt. erwerben. In diesem Fall sammeln wir die eingehenden Beiträge und stellen sie zu 100% für Projekte an Aachener Schulen zur Verfügung (wobei wir Sie über diese Projekte informieren).

Wir werden uns dem Umgang mit Browsern und insbesondere dem Aspekt des Managements und der zentralen Konfiguration auf dem Netzwerk- System- und Service-Management-Forum 2005 stellen.

Dazu dient ein aktueller Vortrag von ComConsult Beratung und Planung über die betrieblichen Unterschiede von Firefox und Internet Explorer. Parallel steht Herr Höchel-Winter am Stand von ComConsult Research bereit, um mit Ihnen die Initiative, den Vortrag zur Anwender-Sensibilisierung und mögliche Nutzungen in Ihrem Unternehmen zu besprechen.

Ihr
Dr. Jürgen Suppan

Schwerpunktthema

VoIP über NAT: Darf's auch etwas mehr sein?

Fortsetzung von Seite 1

Markus Schaub ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbreiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuster Hard- und Software aus dem Netzwerkumfeld.
Insbesondere verfügt er über langjährige Betriebs- und Praxiserfahrung mit CISCO-Routern und CISCO-Switch-Systemen. Er ist ComConsult Certified Network Engineer zertifiziert. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.

In diesem Artikel werden die neuartigen Herausforderungen der Übertragung von VoIP-Traffic über Firewalls und deren Lösungen inkl. ihrer spezifischen Probleme beschrieben.

2 Grundlagen

Das Grundproblem bei der Verbindung zwischen einem LAN und dem Internet ist das Network Address Translation (NAT), welches in der Regel von Firewalls beim Übergang ins Internet vorgenommen wird. Eingeführt wurde NAT primär, um der Adressknappheit von IPv4 entgegenzuwirken. Beim NAT werden die intern genutzten, privaten IP-Adressen gegen öffentliche Adressen ausgetauscht, die im Internet geroutet werden. Da es grundsätzlich möglich ist, bei dem Prozess viele interne IP Adressen auf eine öffentliche abzubilden, benötigt man nur noch wenige IP Adressen, um ganzen Netzwerken den Internet-Zugriff zu ermöglichen. Abbildung 1 zeigt eine schematische Darstellung der Vorgehensweise.

Voraussetzung für fast jegliche Variante von NAT ist, dass die Verbindung wie im Beispiel von Innen nach Außen aufgebaut wird. Hintergrund ist, dass die NAT Tabellen in der Regel dynamisch erstellt werden, was zwar nicht zwingend jedoch üblich ist. D.h. die Zuordnung der intern genutzten Adresse zur öffentlichen IP Adresse findet erst während des Verbindungsaufbaus statt.

Bislang stellte dieses Vorgehen kein Problem dar, da die meisten Verbindungen zwischen Lokalen Netzen und dem Internet in der Tat Client-Server-Verbindungen waren: ein Web-Browser greift auf einen http-Server zu, ein FTP Programm auf einen FTP-Server, ein Telnet-Client auf ei-

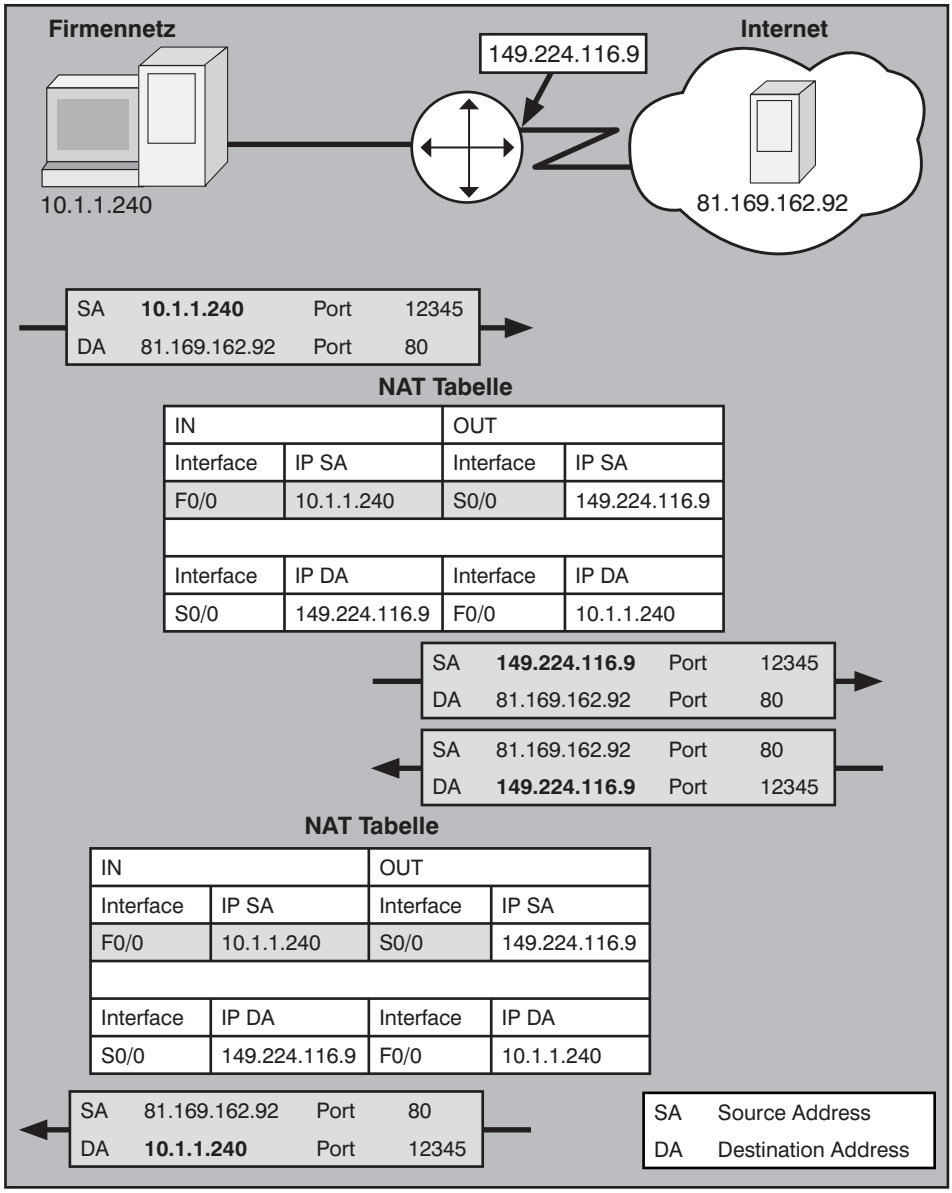


Abbildung 1: Schematischer Ablauf von NAT

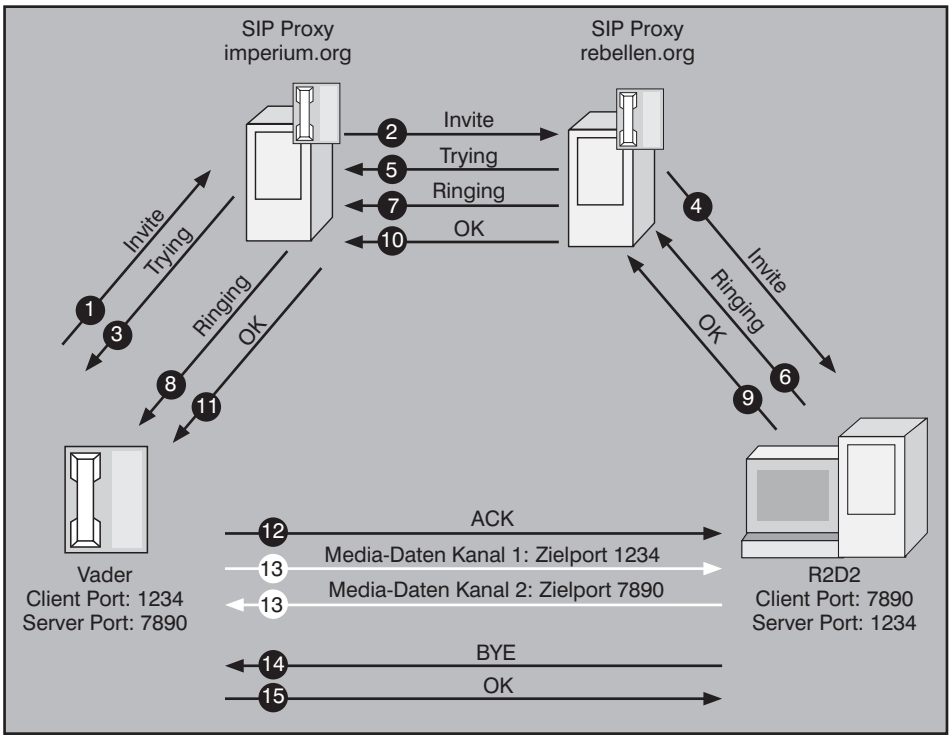


Abbildung 2: SIP Trapez

nen Telnet-Server, etc. Mit der Einführung von VoIP ändert sich das jedoch, aus der gewohnten Client-Server- wird eine Any-to-Any-Kommunikation. Der Datenstrom zwischen den Telefonen läuft nicht mehr über einen Server, sondern direkt von Endgerät zu Endgerät.

Und schlimmer noch: nicht nur reden jetzt Endgeräte direkt miteinander, die Ports sind im Gegensatz zur klassischen Kommunikation nicht mehr vorhersehbar. Bei HTTP weiß man, dass die Verbindung zu Port 80 aufgebaut wird, Port 25 für emails etc. Bei Peer-to-Peer Gesprächen werden die Portnummern jedoch häufig erst beim Verbindungsaufbau von den Gesprächspartnern festgelegt.

Abbildung 2 zeigt beispielhaft den Kommunikationsablauf von SIP, das so genannte SIP-Trapez. Der Verbindungsaufbau läuft noch über dedizierte Server, die SIP Proxies. Nach dem Verbindungsaufbau werden die Daten jedoch direkt von Telefon zu Telefon übertragen. Dazu werden pro Mediastream zwei Kanäle aufgebaut, je einer in jede Richtung. D.h. jedes Telefon ist zugleich Client als auch Server. Aus Sicht von NAT ist dies eine Katastrophe: jedes VoIP Endgerät, sei es Hardphone oder Softphone, muss nun aus dem Internet heraus erreicht werden können. Und schlimmer noch: welche Ports genutzt werden, wird im Verbindungsaufbau ausgehandelt und sie können sich während der Verbindung ändern, wenn beispielsweise nachträglich neben der Sprach- auch noch eine Videoverbindung zugeschaltet wird. Grundsätzlich ist es erlaubt, nahezu jeden Port dafür zu benutzten. Auch wenn viele SIP-Applikationen eine Einschränkung auf einen begrenzten Portrange zulassen, bleibt das generelle Problem doch bestehen.

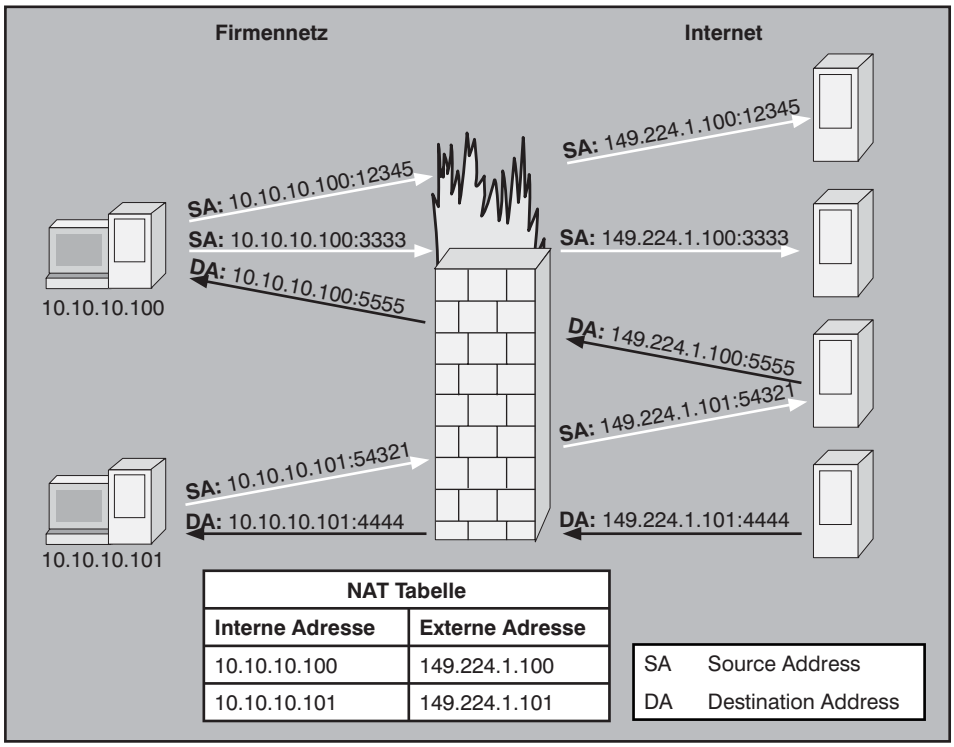


Abbildung 3: Full Cone NAT

Die hier dargestellten Schwierigkeiten zwischen NAT und SIP lassen sich von der Problemstellung her auf andere Any-to-Any-Anwendungen wie H.323 oder Instant Messageing übertragen.

2.1 Varianten des NAT

Ein Problem mit NAT ist die unterschiedliche Nomenklatur, die benutzt wird. Zwar wird im RFC 2663 versucht Klarheit in das Begriffswirrwar zu bringen, jedoch gehört er wohl zu den meistignorierten RFCs, die jemals geschrieben wurden.

Ein Grund dafür ist, dass man NAT von zwei Perspektiven aus betrachten kann: von der Konfiguration und von den Konsequenzen her. Für den Administrator eines NAT-Gateways ist es beispielsweise von entscheidender Bedeutung, ob er die Übersetzungstabelle statisch einrichten muss oder ob sie dynamisch entsteht; ob neben der reinen IP Adresse auch Portnummern beachtet werden oder nicht, was häufig als PAT (Port Address Translation) oder genauer als NAPT (Network and Port Address Translation) bezeichnet wird; usw.

Für einen Anwendungsentwickler hingegen, der Daten über mindestens ein NAT-Gateway übertragen muss, ist es unerheblich, wie die Tabelle zustande kommt. Ihn interessieren viel mehr Fragen wie: bekommt seine Anwendung immer dieselbe externe IP Adresse beim Austausch zuge-

wiesen, oder ändert sich die Portnummer beim Übergang vom privaten ins öffentliche Netz.

Für das Traversal Problem haben sich folgende Begriffe eingebürgert, die vier Varianten bezeichnen, die von Bedeutung sind.

2.1.1 Full Cone
Beim Full Cone NAT wird dieselbe interne IP Adresse immer auf dieselbe externe IP Adresse abgebildet und die Portnummern werden nicht geändert. (siehe Abb. 3) Full Cone setzt somit voraus, dass für jedes interne Gerät eine offizielle IP Adresse existiert, die auf dem NAT-Gateway statisch konfiguriert werden. Stellt sich natürlich die Frage, warum die öffentliche IP Adresse nicht an das Gerät selbst vergeben wird und so auf NAT gänzlich zu verzichten, wenn ohnehin für nahezu jedes interne Gerät eine existiert. Zumeist wird aus Sicherheitsgründen darauf verzichtet.

Klarer Vorteil von Full Cone ist die generelle Vorhersagbarkeit. Verbindungen, die aus dem Internet heraus aufgebaut werden, können problemlos internen Geräten zugeordnet werden. Auch die ausgehandelten, zufälligen Layer-4-Portnummern machen keine Schwierigkeiten, da sie durch das NAT nicht geändert werden.

Die Nachteile liegen jedoch auf der Hand: es werden ungeheuer viele öffentliche IP Adressen benötigt und durch die dynamische Vergabe der Portnummern die Firewall-Funktion de facto ausgehebelt. Zumindest für das zweite Problem wäre ein Application Layer Gateway eine Lösung, das nur für bestimmte Kommunikationen einen Verbindungsaufbau erlaubt. Auf die genaue Funktion eines solchen Gateways wird später noch eingegangen werden.

Konsequenzen für Any-to-Any-Applikationen:

Die interne Applikation muss herausfinden, welche IP-Adresse dem Gerät, auf dem sie installiert ist, im Internet zugewiesen bekommt.

Danach steht einer Any-to-Any-Kommunikation nichts mehr im Wege.

2.1.2 Restricted Cone
Port Restricted Cone unterscheidet sich vom Full Cone nur in einer einzigen Besonderheit: eine Verbindung zu einer bestimmten IP-Adresse muss von innen nach außen aufgebaut werden. Wie beim Full Cone wird jedoch einer internen IP Adresse immer dieselbe öffentliche Adresse eindeutig zugewiesen, dasselbe gilt für die Portnummern. (siehe Abbildung 4)

Die Besonderheit des Restricted Cone NAT ist, dass ein externer Host zu einem internen Host dann eine Verbindung mit anderer Portnummer aufbauen kann, wenn der interne bereits schon einmal mit dem externen kommuniziert hat.

Klingt komplizierter als es ist! Einfacher formuliert: hat ein Rechner aus einem LAN bereits mit einem Rechner im Internet geredet, ist zwischen den beiden Rechnern von da an alles erlaubt. Verboten ist hingegen eine Kommunikation, bei der ein externer Host als erster anfängt zu senden.

Der Vorteil gegenüber dem Full Cone liegt in einer erhöhten Sicherheit.

Ein Nachteil, der geblieben ist, ist die hohe Anzahl an benötigten, öffentlichen IP Adressen. Aus diesem Grund wird dieses Verfahren nur selten eingesetzt.

Konsequenzen für Any-to-Any-Applikationen:

1. Die Applikation muss herausfinden, welche IP Adresse ihr zugewiesen wird. 2. Die Applikation muss als erstes mit der Kommunikation beginnen

Das zweite Problem existiert in der Praxis nicht, da die heute gängigen Peer-to-Peer Anwendungen eine Verbindung zu einem Server halten, an dem sie sich anmelden und den sie benötigen, um die Gesprächspartner zu finden. Bei SIP wären das beispielsweise der Registrar und der SIP Proxy. Bei dem Mediastream muss die Applikation einzig dafür Sorge tragen, dass sie als erstes den Stream zum Gesprächspartner aufbaut. Der Rückkanal ist anschließend ja erlaubt.

2.1.3 Port Restricted Cone
Der Port Restricted Cone ist eine weitere Verschärfung des Restricted Cone: gebliebn ist, dass auch hierbei ein internes IP Address/Port Pärchen auf ein extern genutztes IP Address/Port Pärchen abgebildet wird. Im Beispiel wird die interne IP Adresse 10.10.10.100 mit der Portnummer 12345 gemappt auf die öffentliche IP Adresse 149.224.1.100 mit der Portnummer 54321.

Die Verschärfung im Vergleich zum Restricted Cone liegt darin, dass Verbindungen von außen nur mehr möglich sind, wenn sie von innen begonnen werden. Kommt nun von außen ein Paket für die IP Adresse 149.224.1.100 zum Port 7777, so schlägt die Zustellung fehl. (siehe Abbildung 5)

In der Sprechweise der Administratoren ist Port Restricted Cone eine Variante des NAPT oder PAT. Die Besonderheit ist, dass die IP Adresszuordnung konstant ist, was bei NAPT/PAT nicht zwingend der Fall sein muss. In der Praxis handelt es sich um das NAT, das beispielsweise von den meisten Routern im Home Bereich genutzt wird.

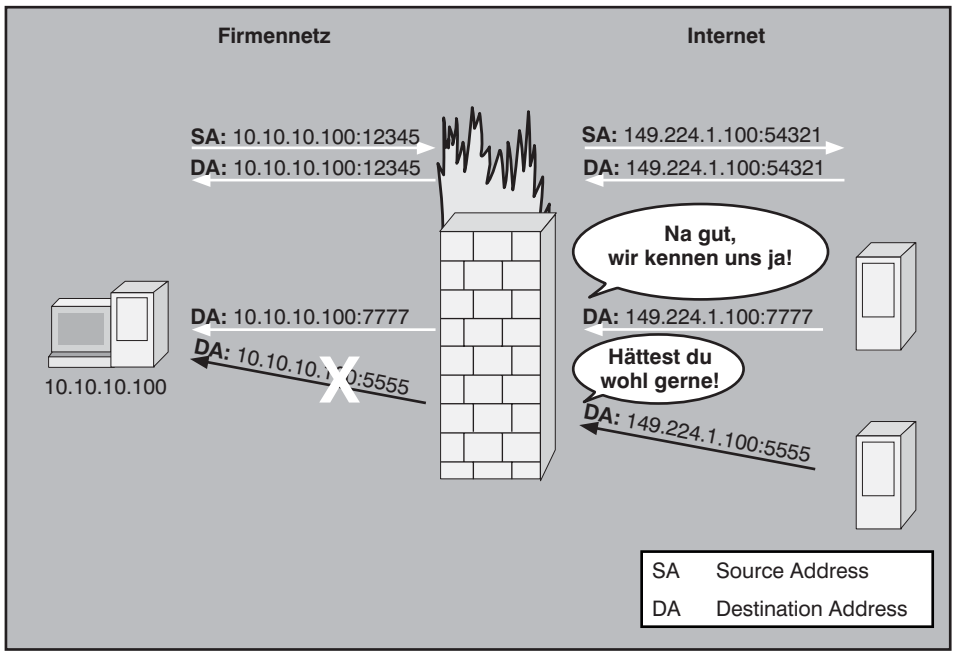


Abbildung 4: Restricted Cone

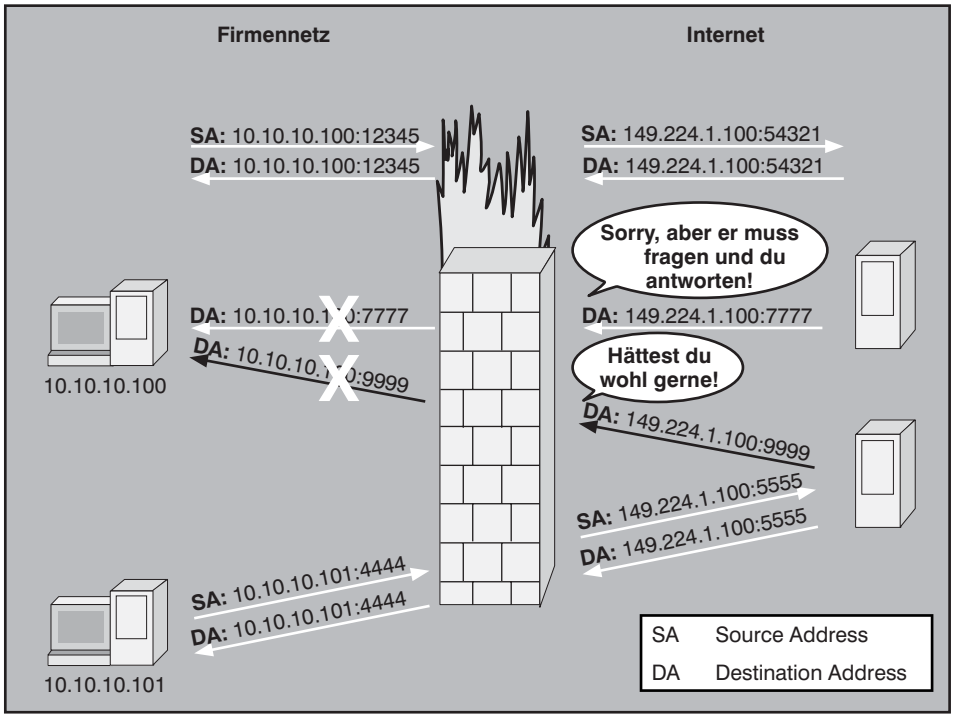


Abbildung 5: Port Restricted Cone

Vorteil dieses Verfahrens ist es, dass es nun möglich ist, mehr als eine interne IP Adresse auf eine einzige öffentliche IP Adresse abzubilden. Das NAT Gateway muss nur dafür sorgen, dass die IP Address/Port Pärchen eindeutig bleiben, nicht mehr, dass die IP Adressen selbst eindeutig einander zugeordnet werden.

Nachteil dieses Verfahrens ist es, dass Verbindungen von außen nach innen nicht aufgebaut werden können. Aus Sicht der Sicherheit kann man das als Vorteil auffassen und bislang wird NAPT auch genau deshalb gerne eingesetzt - neben dem Vorteil der Einsparung von öffentlichen IP Adressen. Im Sinne von Peer-to-Peer Anforderungen handelt es sich jedoch um einen entscheidenden Nachteil.

Konsequenzen für Any-to-Any-Applikationen:

1. Die Applikation muss herausfinden, welche IP Adresse für ihre Pakete im Internet genutzt wird.
2. Das NAT Gateway muss ein Pinhole für die Kommunikation von außen nach innen öffnen.

Die Applikation alleine kann also nichts mehr tun, um die Kommunikation zuzulassen. Es ist notwendig, dass auch die Firewall ihren Beitrag leistet. Auf die Verfahren, die dazu zur Anwendung kommen können, wird später noch eingegangen.

2.1.4 Symetric Cone

Der letzte und aus Sicht von Any-to-Any-Applikationen schwierigste Fall ist das symmetrische NAT. Wie bei Port Restricted NAT werden auch hierbei IP Address/Port Pärchen von dem NAT Gateway dynamisch erzeugt. Jedoch ist diesmal nicht mehr sichergestellt, dass eine interne IP Adresse auch immer dieselbe externe IP Adresse zugewiesen bekommt. Stattdessen ist es möglich, dass bei dem Aufbau einer neuen Verbindung zu einer anderen externen IP Adresse auch eine andere öffentliche IP Adresse bei der Übersetzung durch NAT genutzt wird. Portnummern können sich wie bei Port Restricted NAT ebenfalls ändern. (siehe Abbildung 6)

Im Beispiel wird für die Verbindung zum ersten Server die interne IP Adresse 10.10.10.100 durch die öffentliche IP 149.224.1.100 ersetzt, bei einer weiteren Verbindung zum zweiten Server im Internet wird dieselbe interne IP Adresse jedoch durch die öffentlich Adresse 80.81.82.83 ersetzt.

Schon ist das Problem des Port Restricted Cone allein durch die Applikation nicht mehr zu lösen, sondern setzt spezifische Fähigkeiten der Firewall voraus, so ist das symmetrische NAT für die Applikation zu einem unlösbares Problem geworden.

Konsequenzen für Any-to-Any-Applikationen:

Um symmetrisches NAT einer Firewall zu überwinden, reichen die Bordmittel, die eine Anwendung mitbringen kann, nicht aus.

Trotzdem besteht Grund zur Hoffnung. Später in diesem Artikel werden Lösungen vorgestellt, die das Problem heute schon lösen können.

2.2 Eigentliches Problem: Firewall

Auch wenn das NAT Traversal Problem eines der von den Standards her am meisten diskutierten Probleme ist, stellt es

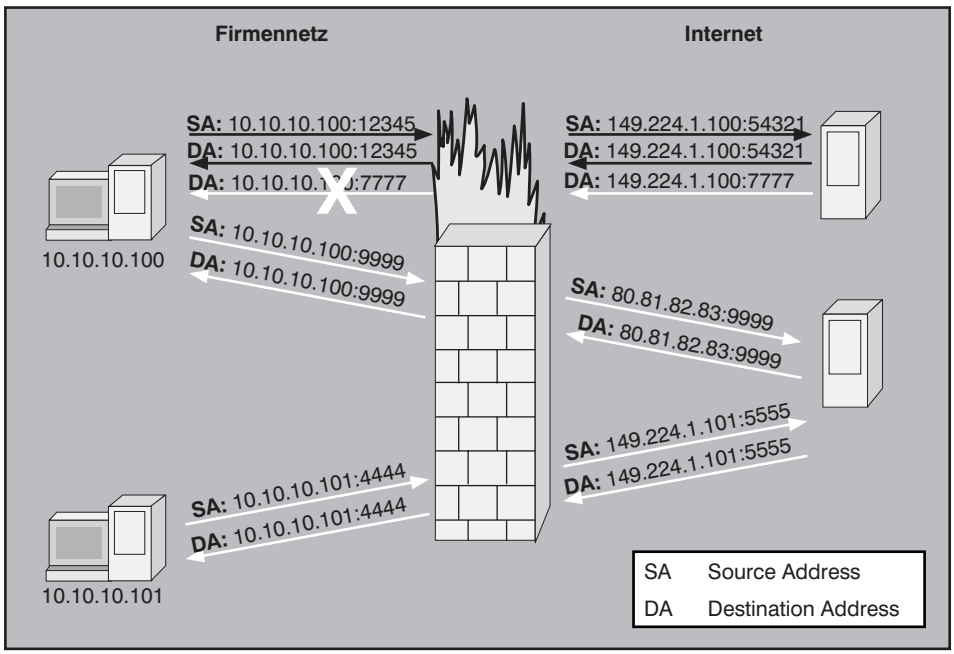


Abbildung 6: Symetric Cone

im Grunde nicht das Hauptproblem dar. Selbst ein Unternehmen, das in der glücklichen Lage ist, über ausreichend öffentliche IP Adressen zu verfügen, um gänzlich ohne NAT leben zu können, würde es trotzdem erhebliche Probleme mit jeglicher Peer-to-Peer-Kommunikation haben, wie sie heute für VoIP vorgesehen ist.

Die beiden Kernproblem sind, dass

- VoIP Anwendungen von außen erreichbar sein müssen
- die Portnummern dynamisch vergeben werden dürfen

Beides widerspricht eklatant den Regeln jeglicher Sicherheitspolitik. Bestandteil von jedem Firewall-Konzept sind so genannte Portfilter, die nur besondere Ports erlauben, alle anderen aber verbieten. Die Pakete, die über erlaubte Ports eintreffen, wiederum können dann an bestimmte andere Programme übergeben werden, die die Pakete ihrem Layer 5-7 Protokoll entsprechend prüfen können. Beispiel: was über Port 80 hereinkommt wird an einen http-Proxy übergeben, der im http-Anteil prüft, ob beispielsweise Java darin ist und es dann ggf. das Paket verwirft.

Die dynamische Vergabe der Portnummer von VoIP Anwendungen hebelt die Portfilter jedoch komplett aus, da alle Ports erlaubt werden müssten. Das wiederum würde in letzter Konsequenz bedeuten, dass wir bei Einführung von VoIP alle unsere Firewalls auf den Müll schmeißen könnten, da die Portfilter nicht mehr anwendbar sind, gäbe es nicht Mittel und Wege, das Problem in den Griff zu bekommen.

2.3 Konsequenzen für VoIP

Wie beschrieben bildet NAT eine natürliche Grenze für jegliche Kommunikation, die vom Internet her aufgebaut werden soll. Zwar erlaubt Full Cone, dass eine Verbindung von außen aufgebaut werden darf, ohne dass ein interner Client zuvor den ersten Schritt getan haben muss, aber selbst in diesem einfachen Fall müsste ein externer VoIP Client wissen, welche Adresse er ansprechen soll. Das ist jedoch genau das Problem: NAT ist von der Idee her transparent für interne Geräte; d.h. eine intern eingesetzte VoIP Applikation kann zunächst einmal nicht wissen, dass die IP Adresse von einem NAT Gateway geändert wird, geschweige denn, welche IP Adresse die Pakete im Internet haben werden.

Die andern NAT Varianten verschärfen das Problem Schritt für Schritt bis hin zum Symetric Cone NAT, wo es noch nicht mal händisch möglich wäre, dem Client die externe IP Adresse mitzuteilen, da der Firewall ein ganzer Pool davon zu Verfügung steht, aus dem sie nach Gutdünken schöpfen kann.

3 Standardlösungen

Jeder der möglichen Lösungsansätze ist komplex genug um einen eigenen Artikel zu rechtfertigen. Darum sollen im Folgenden die heute verfügbaren und die sich am Horizont abzeichnenden Lösungen nicht in ihren technischen Details vorgestellt werden. Stattdessen wird die generelle Funktionalität des jeweiligen Ansatzes vorgestellt und bewertet. Dabei werden zunächst die Lösungen vorgestellt, die entweder schon als RFC vorliegen oder bei der IETF zumindest schon Drafts vorhanden sind. Zuletzt werden noch zwei Herstellerlösungen vorgestellt, die gegenüber den Drafts der IETF den Vorteil haben, bereits in Produktform erhältlich zu sein.

3.1 VPN

Virtual Private Network (VPN) ist eher ein Marketingschlagwort als ein Verfahren. Gemeint ist eine ganze Reihe von Lösungen und Techniken. Den meisten gemeinsam ist die Idee, zwei private Netze über ein öffentliches Netz so miteinander zu verbinden, dass es für Clients innerhalb der privaten Netze so aussieht, als würde es gar kein öffentliches Netz geben. Die Folge davon ist beispielsweise, dass in beiden privaten Netzen auch private IP Adressen genutzt werden können, ohne dass NAT notwendig wäre. Neben der Verbindung ganzer Netzwerke ist mit VPN-Techniken jedoch auch die Anbindung einzelner Client an ein privates Netz möglich, wie sie in der unteren Grafik von Abbildung 7 dargestellt wird.

Typisch für beide dargestellten VPN-Varianten ist ein so genanntes Tunneling: dabei werden die IP Pakete der privaten Netze für die Übertragung über das öffentliche Netzwerk unverändert übertragen. Möglich ist das dadurch, dass sie in öffentliche Pakete eingepackt als „Daten" eines „neuen" IP Paketes übertragen werden.

Das Tunneling umgeht in den meisten Fällen NAT, indem die Firewall entweder zugleich NAT- und VPN-Gateway ist oder aber ein separates VPN-Gateway parallel zum NAT-Gateway an das Internet angeschlossen wird. Die logische Konsequenz ist, dass es kein NAT-Traversal Problem gibt: denn wo kein NAT, da kein Problem mit NAT.

Eine VPN Lösung eignet sich also besonders gut für die Verbindung zweier oder mehrerer Standorte und für die Anbindung mobiler User an ein Firmennetz. Ein Nachteil jeglicher VPN Lösung ist jedoch die erhöhte Latenzzeit, die durch die Verfahren entstehen und bei Delay-kritischen Anwendung ein Problem werden können. Ein anderer Nachteil ist, dass vielfach auch für VPN Verbindungen eine Portbeschränkung der übertragenen Daten besteht. Da viele Voice-Applikationen jedoch gerade mit dynamischen Ports arbeiten, müsste diese Beschränkung aufgehoben werden, was einer Lockerung der Sicherheitspolitik für VPNs vieler Firmen gleichkommt.

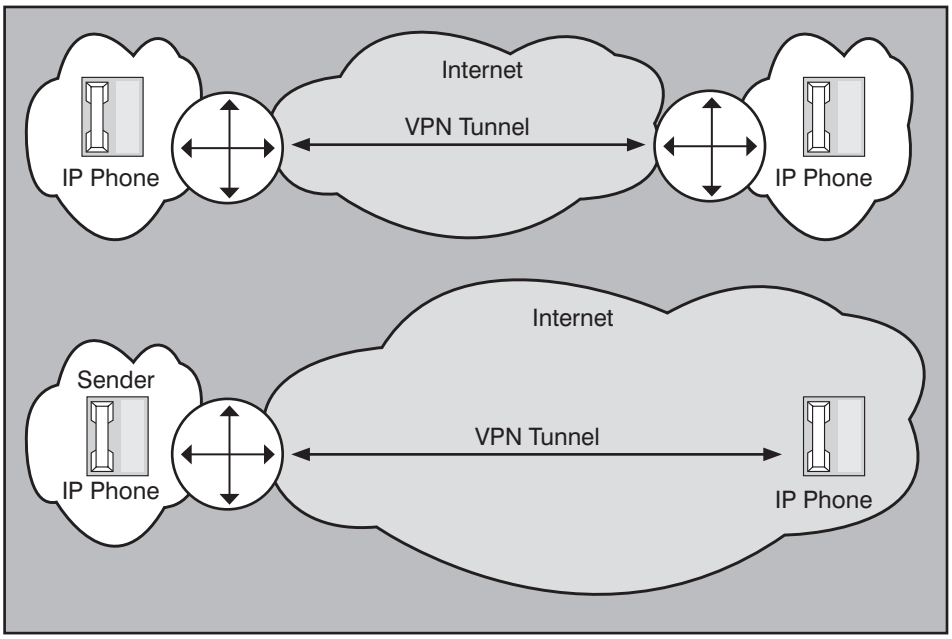


Abbildung 7: VoIP über VPN

Der größte Nachteil jeglicher VPN Technik ist jedoch, dass sie voraussetzt, dass sich beide Enden der Verbindung vertrauen. Damit ist keine Variante von VPN geeignet, VoIP-Anrufe oder andere Peer-to-Peer-Verbindungen von Fremden zuzulassen. Eine generelle Lösung für die VoIP/NAT-Problematik ist VPN also in keinem Fall.

3.2 Einstellen der Ports

Eine typische Lösung für die NAT Problematik, wie sie im SOHO Bereich vielfach zur Anwendung kommt, ist die statische Konfiguration für einkommende UDP Ports. Das NAT Gateway wird dann angewiesen, dass eintreffende Pakete mit spezifischen Portnummern an eine bestimmte interne IP Adresse weitergeleitet werden. Im Beispiel wurde festgelegt, dass Pakete, die mit einem Zielport im Range von 8000 bis 8006 ankommen, an die interne IP Adresse 10.1.1.101 weiter zu leiten sind, ohne dass die Portnummer geändert werden soll. Anders als bei allen anderen eintreffenden Paketen, ist es für diesen Port-Range nicht erforderlich, dass die Verbindung von innen heraus aufgebaut wurde. In der Sprechweise der NAT-Konventionen handelt es sich für die Ports 8000-8006 also um ein Full Cone NAT. Die restlichen Verbindungen hingegen werden typischerweise als Restricted Port Cone abgewickelt.

Damit das Verfahren funktioniert sind zwei Voraussetzungen erforderlich:

1. Der interne VoIP-Client (im Beispiel das IP-Phone) muss die IP Adresse kennen, die extern genutzt wird. Klassischerweise also die IP Adresse, die dem DSL Router bei der Einwahl vom Provider für das DSL-Interface zugewiesen wurde.

2. Die Ports für die VoIP Anwendungen müssen bekannt sein, damit sie auf dem DSL-Router eingestellt werden können.

Die zweite Voraussetzung lässt sich in der Regel leicht bewerkstelligen, da Anwendungen für den Home-Bereich mit festen Port-Ranges arbeiten, die entweder auf dem Client einstellbar sind oder vom Hersteller zwar fest vorgegeben aber bekannt sind.

Um die erste Bedingung zu erfüllen, gibt es einige Möglichkeiten:

1. Manueller Eintrag der externen IP Adresse beim Client
   Diese Lösung ist bei vielen Peer-to-Peer Anwendungen möglich, jedoch ist sie ausgesprochen umständlich und Anwender-feindlich.

2. Automatische Discovery der extern genutzten Adresse
   Der Client ist in der Lage herauszufinden, welche IP Adresse seine Pakte nach dem NAT haben. Dafür gibt es für VoIP ein mittlerweile gängiges Verfahren, STUN, auf das später noch eingegangen wird.

3. Dynamisches DNS
   Anstatt seiner IP Adresse gibt der Client seinen DNS-Namen bekannt. Die Gesprächspartner werden vor dem Verbindungsaufbau also die IP Adresse beim DNS erfragen müssen. Der Router wiederum ist so konfiguriert, dass er mittels dynamischem DNS bei jeder IP Adressänderung seinen DNS Eintrag entsprechend ändert.

Alle drei vorgestellten Verfahren sind heute bei verschiedenen Peer-to-Peer Verfahren üblich. Welches sich für welche Applikation am besten eignet oder anwendbar ist, hängt zumeist von der Art der Anwendung und der konkreten Applikation ab.

Die statische Weiterleitung fester Ports hat jedoch ihre Grenzen in der Anwendbarkeit: ist sie im SOHO Bereich vom Aufwand her noch vertretbar, so stößt sie bei größeren Installation schnell an ihre Grenzen. Doch auch im Home-Bereich gibt es Nachteile: für die Konfiguration muss der Anwender zumindest rudimentäre Kenntnisse über IP besitzen. Somit wird sie in vielen Fällen nur von einem recht kleinen Kreis von Usern angewendet werden können. Ein weiterer Nachteil ist, dass die einmal geöffneten Ports dauerhaft offen bleiben. Unter Security Gesichtspunkten ein KO Kriterium.

3.3 Application Layer Gateway

Die beiden Nachteile der fixen Portkonfiguration sind die Inkompatibilität mit einigen Anwendungen, die auf dynamische Ports „bestehen" und die Einschränkung auf kleine Netzwerke. Diese beiden Nachteile gelten für die Application Layer Gateways (ALG) in weitaus eingeschränkterem Maße. (siehe Abbildung 9)

Die Idee des ALG ist es, einer Firewall mehr beizubringen, als nur bis zu den UDP/TCP Ports zu schauen. Stattdessen bringt man ihnen die Standardprotokolle bei, so dass sie auch auf Grundlage von Applikations-Daten Entscheidungen treffen können. Teilweise wird das auch als „Proxy"-Funktionalität bezeichnet; die Begriffe sind im Firewalling-Umfeld eben so schwammig wie beim NAT. Für Protokolle wie HTTP oder FTP gibt es in den gängigen Firewalls diese Funktion schon lange.

Das Vorgehen eines ALG für SIP oder auch H.323 ist, dass man die Firewall die Signalisierungsdaten mitlesen kann und gemäß den darin ausgetauschten Informationen handelt. Bei SIP beispielsweise würde das ALG die Informationen des SDP mitlesen und so erkennen, wann eine Verbindung aufgebaut werden soll und welche Portnummern die beiden Gesprächspartner für die Mediastreams aushandeln. Das ALG geht nun proaktiv hin und generiert dafür entsprechende NAT Einträge, noch bevor

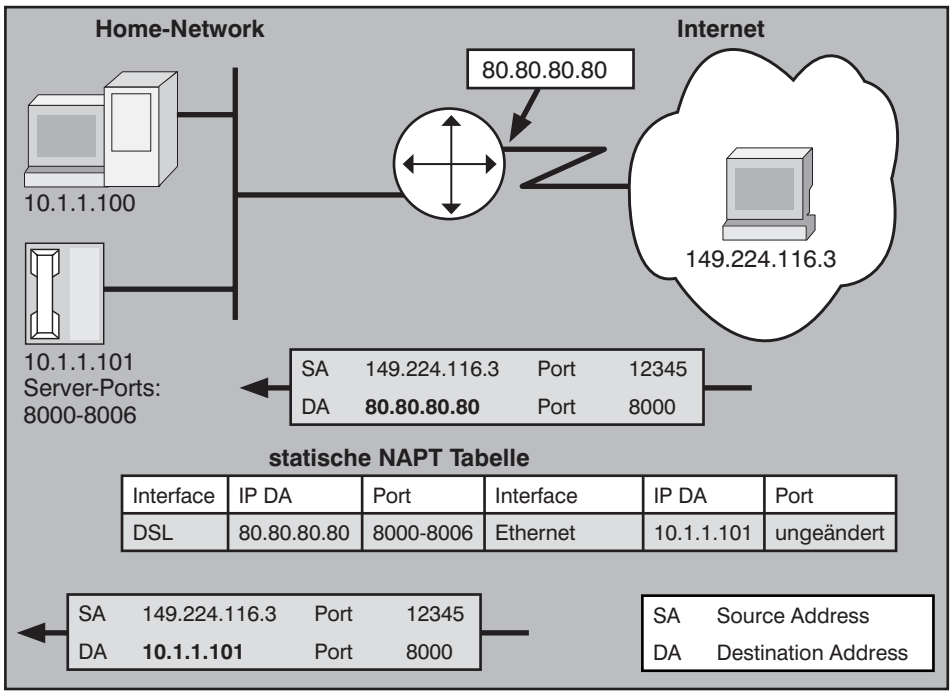


Abbildung 8: Statische Port-Konfiguration

die Verbindung zu Stande kommt. Anders formuliert: das ALG öffnet dynamisch Ports für Verbindungen, von denen es weiß, dass sie in Kürze rechtmäßig aufgebaut werden.

Da das ALG durch die Signalisierung auch über das Ende einer Verbindung Bescheid weiß, können die Ports auch wieder geschlossen werden.

Neben der erhöhten Sicherheit gegenüber statisch geöffneten Ports gibt es eine Reihe weiterer Vorteile. So ist es mit ALGs möglich, auch größere Netzwerke mit geringem administrativem Aufwand an das öffentliche Netz in Bezug auf VoIP anzuschließen. Ferner kann das ALG zumindest das Signalisierungsprotokoll auf zulässige Parameter untersuchen und nötigenfalls korrigieren/blockieren, wenn es Angriffe erkennt. So wie das bei FTP/HTTP/TELNET/etc. heute bereits üblich ist.

Es gibt jedoch auch Nachteile. Allen voran ist dabei das Problem, dass das ALG die Signalisierung verstehen muss. Für Standardprotokolle wie SDP oder die H.323 Suite ist das noch einfach zu bewerkstelligen, jedoch entwickelt sich der Multimedia-Bereich gerade mit einer so hohen Eigendynamik, dass die Standards alleine nicht ausreichen und viele Hersteller auf propietäre Erweiterungen oder gar eigene Signalisierungsprotokolle zurückgreifen. Da ein ALG diese Erweitungen und Protokolle jedoch nicht verstehen kann, versagt diese Lösung in diesen Fällen gänzlich.

3.4 Universal Plug'n'Play

Universal Plug and Play (UPnP) ist eine weitere Möglichkeit, das Problem im SOHO-Bereich zu lösen. Voraussetzung dafür ist, dass sowohl die internen Rechner wie auch der NAT Router das Verfahren unterstützen. Eine detaillierte Beschreibung des UPnP Verfahrens ist nicht Inhalt dieses Artikels, weswegen es hier bei einer schematischen Darstellung des Ablaufs bleibt. (siehe Abbildung 10)

Zunächst muss der Anwendung die interne IP Adresse und die Funktion des Routers bekannt sein. Dieser Schritt ist in der Abbildung 10 nicht dargestellt, gehört jedoch ebenfalls zum UPnP Verfahren dazu. Danach erfragt die Peer-to-Peer Anwendung via UPnP die extern zugewiesene IP Adresse des Routers (im Beispiel: 80.80.80.80). Mit dieser IP Adresse registriert sie sich beim SIP-Server und gibt sie auch über SDP dem Gesprächspartner bekannt. Da die Anwendung weiß, wann sie mit einer Verbindung zu rechnen hat, kann sie zuvor dem Router bekannt geben, welche Ports er öffnen soll und ihm gleichzeitig den Befehl erteilen, Pakete,

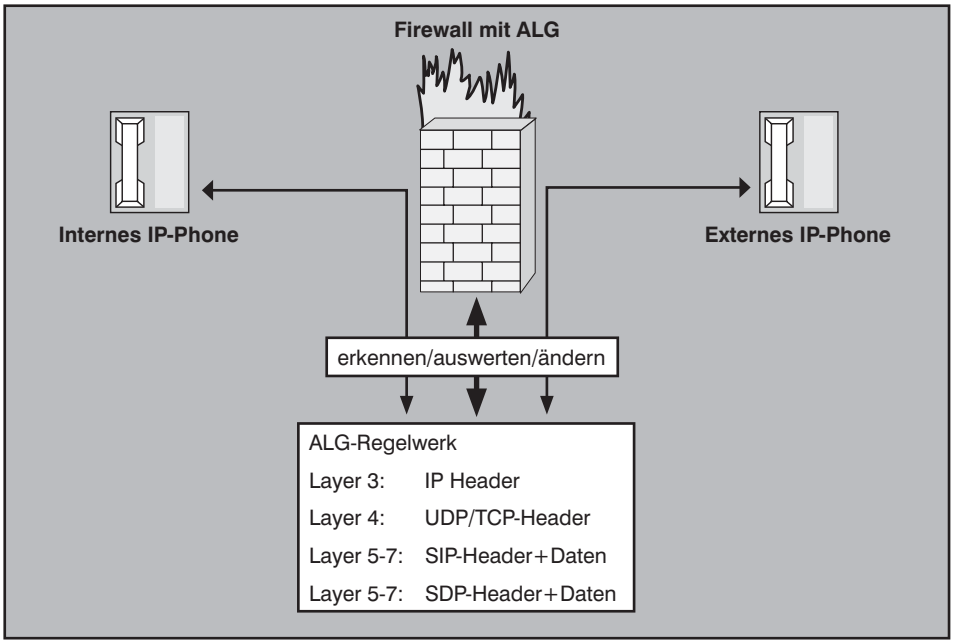


Abbildung 9: NAT Firewall mit ALG

die für diese Ports eintreffen, an sie weiter zu leiten. Wird eine Verbindung beendet, gibt die Anwendung dem Router das ebenfalls bekannt, damit die Ports wieder geschlossen werden.

Im Grunde ist das Verfahren der zuvor vorgestellten statischen Konfiguration von Ports sehr ähnlich, der große Unterschied liegt in der dynamischen Konfiguration des Routers durch die Applikation.

Vorteile von UPnP sind, dass die Ports kurz vor der Kommunikation geöffnet und nachher wieder geschlossen werden, und dass der User sich um nichts kümmern muss. Letzteres macht das Verfahren für die Hersteller attraktiv, da sie so ei-

nen größeren Kreis von Nutzern erreichen können.

Nachteile hingegen sind, dass es klar für den Heimbereich gedacht ist. Große Netzwerke werden so nicht betrieben werden können. Hinzu kommt, dass viele dem UPnP aus Überlegungen der Sicherheit skeptisch gegenüber stehen, wer möchte schon seine Firewall von irgendwelchen Anwendungen „fernkonfigurieren" lassen. Und last but not least: das Verfahren eignet sich nur, wenn es keine NAT-Kaskade gibt. Da die Anwendung nur den ersten NAT Router abfragen kann, kann sie nicht erkennen, dass diese IP Adresse erneut durch ein weiteres NAT geändert wird, bevor die IP Pakete das Internet schlussendlich erreichen.

3.5 MIDCOM

Dem UPnP ähnlich ist ein Standardansatz bei der IETF: MIDCOM (Middlebox Communication). Auch hier ist die Idee, dass die Firewall von einem internen Gerät gesteuert wird, das Kenntnis über die Datenströme hat. Der Unterschied im Vergleich zur UPnP Lösung ist, dass das MIDCOM Verfahren für Unternehmen konzipiert wurde: die Steuerung wird nicht von den Endgeräten, sondern von einem zentralen Kommunikationsserver vorgenommen.

Abbildung 11 zeigt, wie sich die Schöpfer das Prozedere im Falle von SIP vorstellen: da bei SIP die Signalisierung immer über die SIP Proxies läuft, wird einer davon hinter der Firewall platziert, an dem sich die internen Clients registrieren. Wird nun eine Verbindung aufgebaut, so bekommt der SIP Proxy sämtliche Signalisierungspakete, die er auswerten kann. Anhand der SDP Informationen erkennt er, welche Ports der interne Client dem externen anbietet. Daraufhin übermittelt er Steuerbefehle an die Firewall, die diese anweisen, die entsprechenden Ports frei zu schalten und eintreffende Pakete an den internen Client weiterzuleiten. Nach Beendigung des Gesprächs sendet der SIP Proxy der Firewall den Befehl, die Ports und Weiterleitungen wieder zu löschen.

Ein klarer Nachteil der MIDCOM Lösung ist ihre Nichtexistenz. Jedoch ist bei der IETF seit diesem Jahr wieder erkennbar, dass ernsthaft daran gearbeitet wird. Bis Februar gab es nur zwei „Absichts"-RFCs, wie ein solches Verfahren aussehen sollte (RFC 3303) und welche Voraussetzungen bestehen (RFC 3304), beide aus dem Jahr 2002. Im Februar und Juni diesen Jahres sind jedoch zwei weitere dazu gekommen: RFC 3989 beschreibt den Kommunikationsablauf und in RFC 4097 werden bereits potenzielle Kandidaten für das MIDCOM Protokoll begutachtet und bewertet. Eine Entscheidung ist bislang noch nicht getroffen. Im Gespräch sind Protokolle wie SNMP, RSIP, Megaco, Diameter und COPS.

Ansonsten bietet diese Lösung einige Vorteile:

- Durch die zentrale Steuerung über den Signalisierungsserver ist es nicht notwendig, dass die Firewall selbst die Signalisierungsprotokolle versteht. Auch propietäre Protokollerweiterungen wie sie beispielsweise von Microsoft genutzt werden, können problemlos eingebunden werden: da der Microsoft Server die Protokolle ohnehin verstehen muss und dieser dann die Steuerung der Firewall übernehmen kann.

- Ein oder wenige MIDCOM Server sind sehr viel einfacher zu administrieren und zu überwachen als wenn, wie bei UPnP, jedem Rechner und jedem Hardphone das Recht eingeräumt würde, Änderungen an der Firewall-Konfiguration vorzunehmen.

- Die externe IP Adresse müsste nun nicht mehr allen Clients bekannt sein, da diese sich mit der internen an „ihrem" Server registrieren. Der Server muss dann allerdings bei der Signalisierung die IP Adressen im SDP ändern.

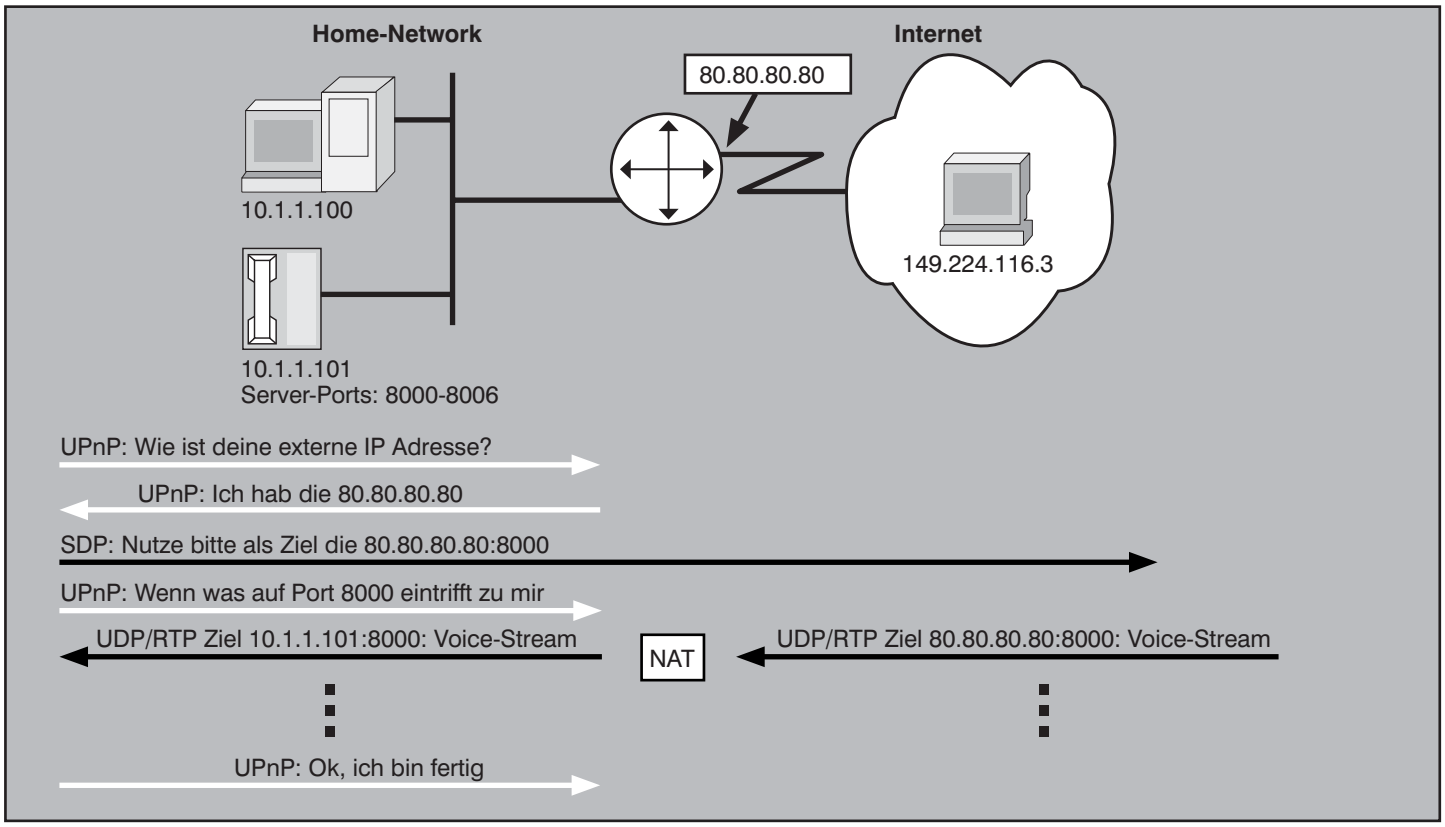


Abbildung 10: NAPT mit Universal Plug'n'Play

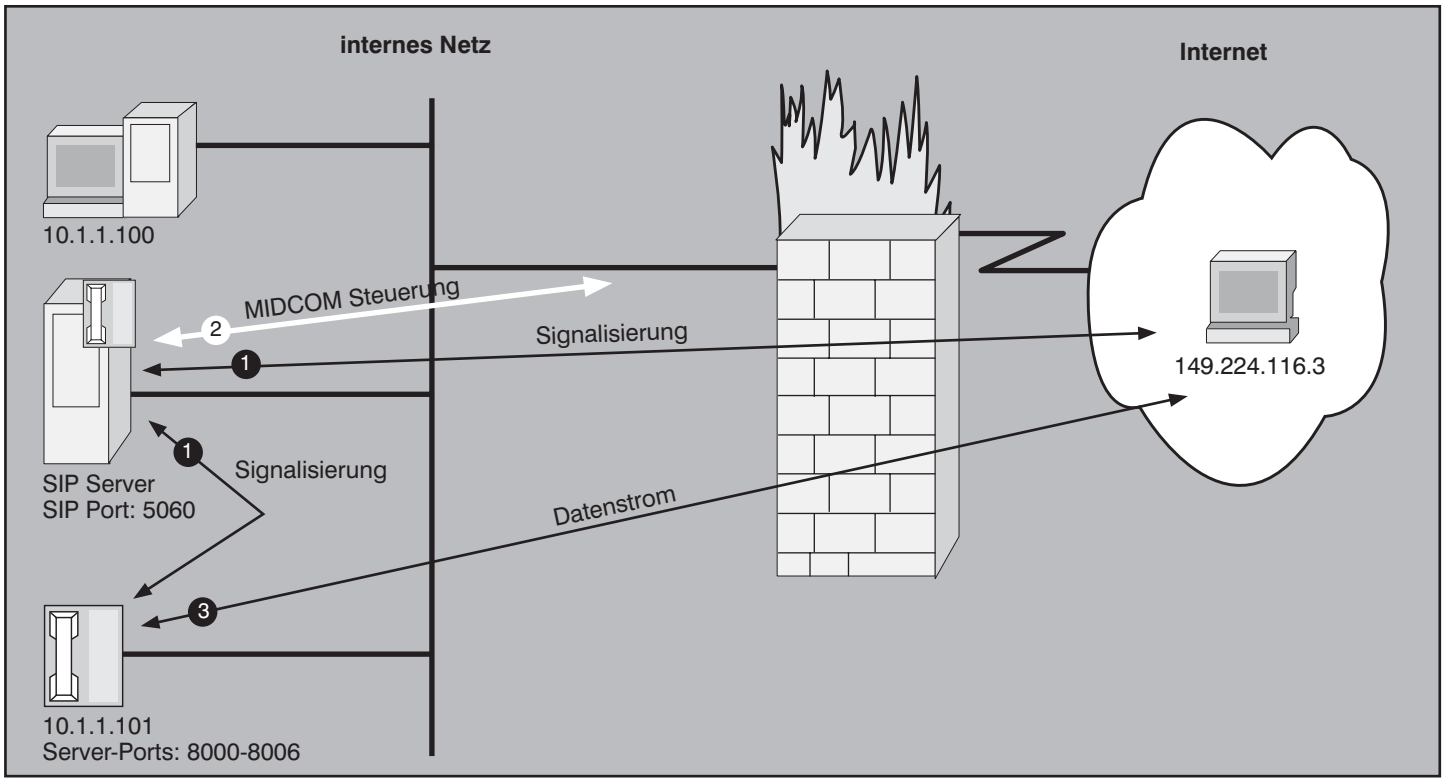


Abbildung 11: NAT Traversal mittels MIDCOM

- Das MIDCOM Protokoll ist nicht auf Sprachkommunikation beschränkt, sondern kann auch für andere Protokolle und Zwecke genutzt werden.

3.6 STUN

STUN, RFC 3489 (Simple Traversal of User Datagramm Protocol (UDP) Through Network Address Translators (NATs)), wendet sich der Ermittlung der externen IP Adresse zu. Ein Problem, das auch bei den bereits beschriebenen Verfahren außer UPnP gelöst werden muss. (siehe Abb. 12)

Die Idee ist recht simpel: um die IP Adresse herauszufinden, die durch NAT im Internet sichtbar ist, sendet die Applikation gleich nach ihrem Start ein Testpaket zu einem STUN Server. Von dessen Existenz weiß er entweder durch einen speziellen Eintrag in seiner Konfiguration oder er hat es via DNS gelernt. Der Server schickt daraufhin die gesehene IP Adresse an den Client zurück. Dadurch kennt der Client nun die IP Adresse, mit der er sich beispielsweise bei einem SIP Server registrieren muss.

Der Standard geht jedoch erheblich weiter. Wie bereits beschrieben gibt es verschiedene Varianten von NAT. Für ein Full Cone NAT wäre dieses einfache Verfahren ausreichend, für ein Restricted Cone und Port Restricted Cone NATs hingegen müsste der Client auch die Portnummern kennen. Aus diesem Grund ermittelt der Client nicht nur die extern genutzte IP Adresse sondern auch die NAT Variante. Dazu sendet er nicht ein einzelnes Paket sondern mehrere Pakete mit unterschiedlichen Portnummern an mindestens zwei verschiedene externe IP Adressen / STUN Server. Auf diese Weise kann er herausfinden, ob ihm immer dieselbe IP Adresse zugewiesen wird, egal mit wem er kommuniziert, und ob sich die Port Nummern ändern. Zuletzt kann er die STUN Server sogar anweisen ihm Pakete auf Portnummern zuzusenden, die er selbst noch nicht als Quellports genutzt hat, um zu sehen, ob Restricted oder Port Restricted Cone vorliegt.

Kommt der Client zu dem Ergebnis, dass es sich um Full oder Restricted Cone handelt, kann er sich mit der gelernten IP Adresse am SIP Server anmelden. Bei Port Restricted Cone weiß er, dass er keine Pakete empfangen würde, die an seinen eigenen SIP-Server Port gesendet werden. Jedoch könnte die Applikation hingehen und versuchen den Port „freizuschießen", indem sie ein UDP Pakte mit dem Port als Absendeport an den Gesprächspartner sendet und so einen entsprechenden, dynamischen NAT Eintrag erzeugt. Oder aber der User könnte den Port auf dem NAT Gateway statisch zur Weiterleitung konfigurieren. Bei symmetrischem Cone hingegen hat die Applikation verloren. Dieses Problem ist mit STUN nicht zu lösen.

Der Vorteil dieses Verfahren ist, dass es sehr einfach und bereits etabliert ist. Für den SOHO Bereich ist das Verfahren in Kombination mit der statischen Portweiterschaltung eine elegante Lösung, die auch in der Breite der VoIP Anbieter und vorhandenen VoIP Clients bereits unterstützt wird.

Im B2B Bereich ist STUN jedoch problematisch. Die Kombination mit der Portweiterschaltung taugt nicht, wie bereits beschrieben. Wo STUN jedoch weiter hilft, ist in Kombination mit einem ALG.

Ein generelles Problem hat STUN jedoch: letzten Endes läuft es nicht auf eine „Ermittlung" der NAT Varianten hinaus sondern auf ein intelligentes „Erraten" derselben. Beispiel: Der Client sendet beim Start mehrere Pakete an seine beiden STUN Server und erhält immer dieselbe IP Adresse zurück. Je nachdem was er sonst noch herausfindet, geht er also von Full, Restricted oder Port Restricted Cone aus. In Wirklichkeit ist es jedoch symmetrisches Cone. Die Fehlannahme leitet sich daraus ab, dass in der Firewall ein Pool von öffentlichen IP Adressen konfiguriert wurde, die sie benutzten darf. Dieses arbeitet sie der Reihe nach ab. Soll heißen, solange NAPT funktioniert, bleibt sie bei der ersten IP Adresse des Pools, erst wenn das nicht mehr ausreicht, nutzt sie

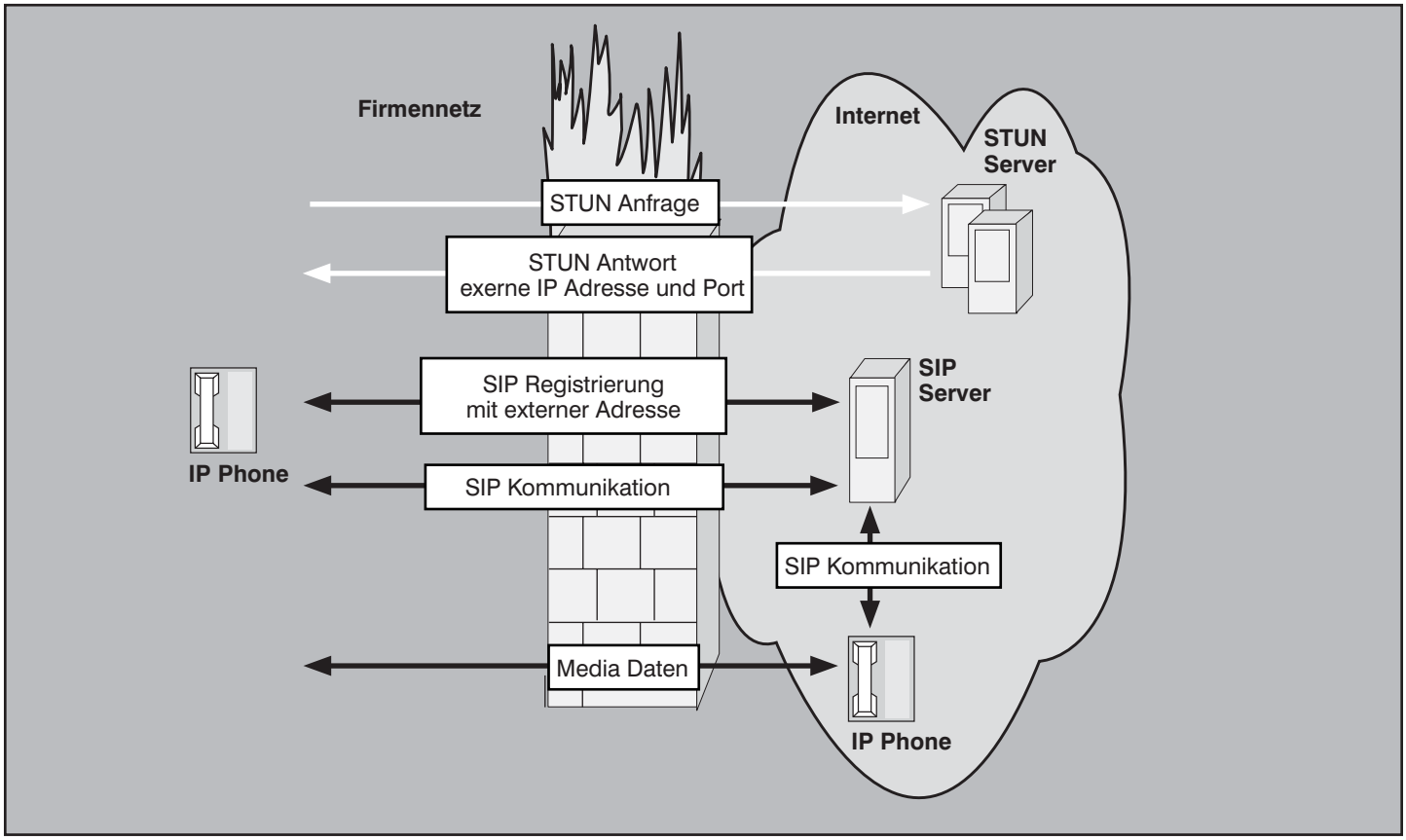


Abbildung 12: STUN

die nächste des Pools. Die Folge wäre, dass beim STUN Test immer dieselbe öffentliche IP Adresse zur Anwendung kommt, da die Pakete kurz aufeinander folgen, später beim Verbindungsaufbau ist es jedoch zum „Überlauf" gekommen und eine andere IP Adresse kommt zum Einsatz.

Dieses systemimmanente Problem sollte bei der Konfiguration der Firewall bedacht werden, will man STUN einsetzen.

3.7 TURN

TURN ist ein mehrstufiges Verfahren. In der ersten Stufe gilt es für den Client zu ermitteln, ob es überhaupt einen TURN-Server gibt und wenn ja, wie er ihn erreichen kann. Grundsätzlich sind dazu zwei Möglichkeiten vorgesehen: erstens, der oder die Server werden konfiguriert; zweitens, es gibt einen speziellen SRV Eintrag im DNS Server, über den der Client die IP Adresse/n des/der Server herausfinden kann. (siehe Abbildung 13)

Sobald der Client den TURN Server kennt, meldet er sich dort an. Da es sich beim TURN-Verfahren um ein Relaying von Paketen handelt, ist die Anmeldung und Authentisierung, anders als bei STUN, nicht optional sondern zwingend erforderlich.

VoIP über NAT: Darf's auch etwas mehr sein?

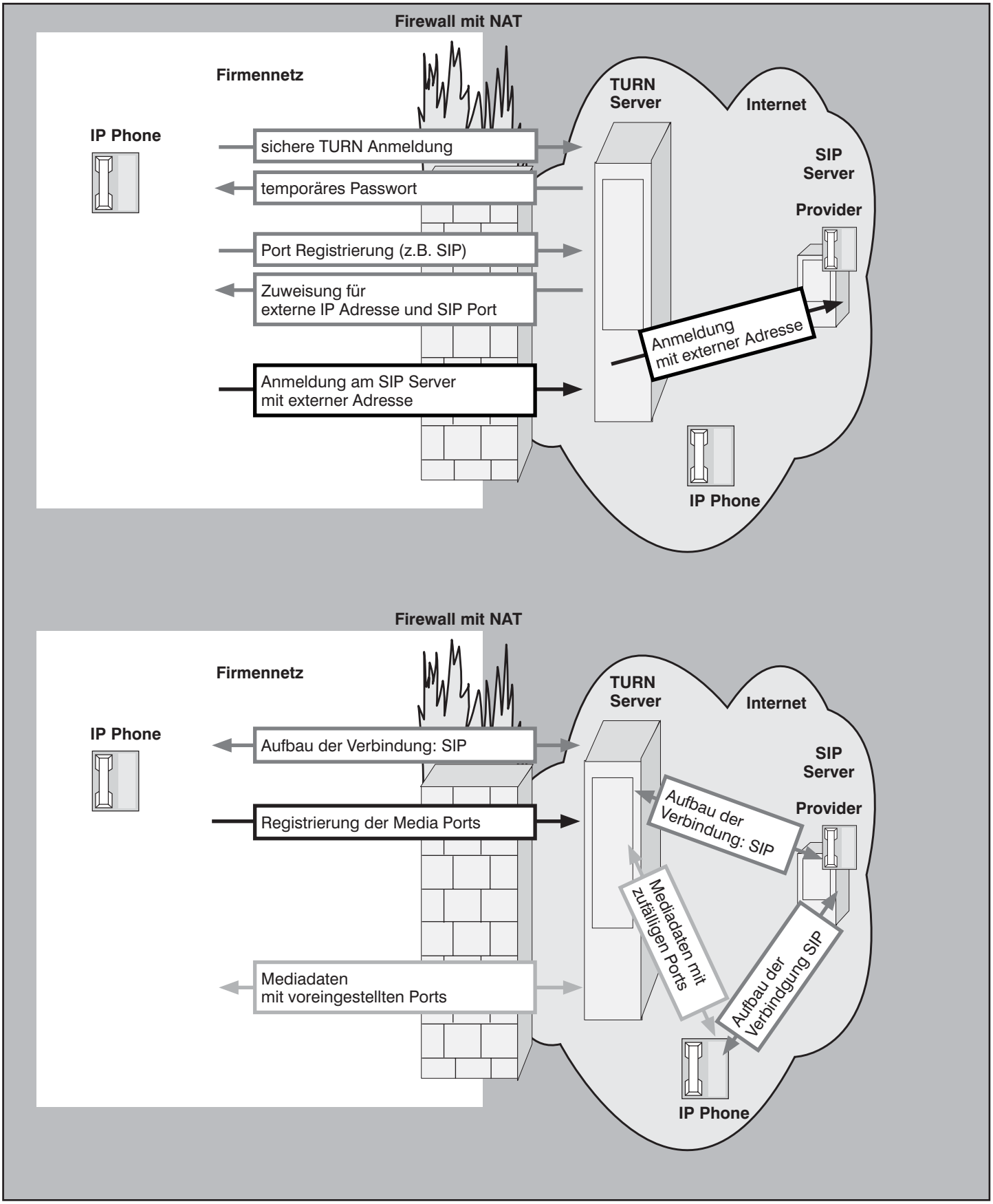


Abbildung 13: TURN

Denn zum einen geht es um die aktive, auf Dauer angelegte Nutzung von Ressourcen, und zum anderen taucht bei den Gesprächspartnern die IP Adresse des TURN-Servers auf. Zwei Dinge, von denen der Betreiber eines Servers sicherstellen will, dass nicht jeder X-beliebige sie nutzen kann.

Nach der erfolgreichen Anmeldung bekommt der Client ein temporäres Passwort zugewiesen, das bis zur Abmeldung zur Authentisierung aller Pakete vom Client an den TURN-Server genutzt wird. Das gilt sowohl für die direkte Kommunikation mit dem Server, wie auch für Pakete, die weitergeleitet werden sollen.

Als nächstes meldet der Client alle Ports an den Server, auf denen er von außen erreichbar sein will. Der Server wird Pakete, die bei ihm auf diesen Ports aus dem Internet eintreffen, an den Client weiterleiten. Bei SIP wäre das im ersten Schritt der Port, der für die Signalisierung genutzt wird, bspw. 5060.

Daraufhin bekommt der Client vom Server die öffentliche IP Adresse genannt, die der Server ihm zur Verfügung stellt, also die, die aus dem Internet heraus erreichbar ist. Der Server pflegt eine TURN-Datenbank, die analog zu einer NAT Tabelle funktioniert: er merkt sich, welcher Client, welche Ports registriert hat und welche IP Adress/Port Pärchen er dafür offen hält. Damit weiß er, wie von extern nach intern zu übersetzten ist.

Jetzt kann der Client diese Informationen für die Kommunikation nutzen. Im Beispiel: für die Anmeldung an einem externen SIP Server. Kommt es nun zu einem Anruf, so wiederholt der Client den Vorgang der Port-Anmeldung am Server für die Mediastreams, bevor er seinem Gesprächspartner die entsprechenden Portnummern und IP Adressen via SDP mitteilt. Wie bei der SIP Signalisierung durchlaufen auch sämtliche Media-Pakete den TURN-Server, der die notwenigen IP Adress- und Portänderungen vornimmt.

Der Trick liegt nun darin, dass die zufälligen Portnummern, des Mediastreams, die aus dem Internet bei dem TURN-Server eintreffen, von diesem geändert werden können. Da die Ports zwischen internem Netz und dem Server voreingestellt werden können, ist es ausreichend, nur diese Ports auf der Firewall frei zu schalten und den Empfang zudem auf die IP Adresse des TURN Server einzuschränken.

Nach Beendigung der Verbindung meldet der Client dem Server, dass die öffentlichen Ports der Mediaverbindung nicht mehr benötigt werden, und der Server sperrt diese daraufhin wieder.

Das TURN Verfahren eignet sich gut, um Symmetric Cone NAT zu überwinden: da der Client nur noch mit einem Server im Internet kommuniziert, dem TURN-Server, bleibt die IP-Adressbindung konstant und ändert sich nicht, wie es beim symmetrischen NAT möglich ist, wenn ein Client mit einem anderen Server kommuniziert. Aus Sicht der internen Sicherheit hat man allerdings nur vergleichsweise wenig gewonnen: ein TURN Server ist kein ALG oder Media-Gateway. Mit anderen Worten, ein TURN Server ändert zwar IP-Adressen und Portnummern, jedoch liest er die Applikationsdaten in den Paketen nicht mit. Somit ist er nicht in der Lage, Angriffe zu erkennen, die über den Application-Layer erfolgen, sondern er verfährt nur wie ein Portfilter, der Pakete zu Verbindungen verwirft, die nicht von einem internen Client begonnen und am Server registriert wurden. Die Schöpfer des Verfahrens fassen das in dem Satz zusammen, dass das TURN Verfahren Symetric Cone in Port Restricted Cone NAT „turned".
Auch wenn TURN mit klarem Blick auf SIP geschaffen wurde und aktuell nur für UDP spezifiziert ist, ist jedoch offensichtlich, dass eben wegen der fehlenden Fähigkeit, die Layer 5-7 Informationen auszuwerten, sich das Verfahren für jegliche Art von Anwendung eignet, für die Symetric NAT ein Problem darstellt. Sogar eine Anpassung für TCP ist trivial möglich und wohl nur eine Frage der Zeit.

TURN hat jedoch noch eine Reihe weiterer Nachteile, die beiden gravierendsten sind wohl zum einen, dass die Ressourcen des Servers naturbedingt begrenzt sind und dass das Verfahren sehr aufwendig ist. Somit kann von einem Server nur eine begrenzte Anzahl von Clients bedient werden. Zum anderen, dass das Verfahren noch Zukunftsmusik ist: weder existieren Server oder Anwendungen, die TURN unterstützen, noch ist der Standard fertig.

Ein paar Worte zum Standardentwurf: aktuell ist der Zustand des Drafts bei der IETF unklar: zum einen gibt es einen Version vom 9.9.2005, die jedoch laut IETF Datenbank seit dem 2.9. auf „dead" gesetzt wurde - man beachte: eine Woche vor ihrem Erscheinen. Auf der Homepage der Arbeitsgruppe taucht der Draft nicht auf. Das alles deutet darauf hin, dass man TURN aufgegeben hat. Andererseits bezieht sich jedoch der neueste ICE Draft vom 21.10.2005 (s.u.), an dem zumindest ein Autor von TURN ebenfalls mitwirkt, häufig auf den TURN Draft. Was dafür spricht, dass der Eintrag in der Da-

tenbank falsch ist.

Der Autor dieses Artikels vermutet, dass die neueste Version des TURN-Drafts eine Woche zu spät abgegeben wurde und vorher Automatismen in der IETF Datenbank zugeschlagen haben, die den Standard wegen fehlendem Updates für tot erklärten. Wahrscheinlich gilt für TURN der berühmte Satz, dass Totgesagte noch ein langes Leben vor sich haben.

3.8 ICE

Alle Lösungen des NAT/VoIP-Problems haben ihre Stärken und ihre Schwächen. Keine davon ist die universelle Lösung, weshalb auch alle ihre Berechtigung haben. Doch leider stellt die Vielzahl unterschiedlicher Lösungen ein Problem in sich dar, da einige der Ansätze sich gegenseitig ausschließen. Beispiele dafür wären:

- Interne Kommunikation schließt STUN aus, denn würde das Telefon die externe IP Adresse der Firewall einem anderen internen Gesprächsteilnehmer als Zieladresse nennen, käme keine Kommunikation zustande.

- Aus dem gleichen Grund schließen sich VPN und TURN, VPN und STUN paarweise aus.

- Auch TURN und STUN stehen im Widerspruch zueinander, da ein Client entweder die Adresse der Firewall oder die des TURN Servers angeben muss.

Um dieses Dilemma zu lösen, gibt es eine weitere Vorgehensweise in der Normung: ICE (Interactive Connectivity Establishment). Aktuell noch im Draft-Stadium schickt sich der Autor an, ein Kommunikationsprofil zu entwickeln, mittels dessen die verschiedenen Verfahren miteinander kombiniert werden können. Interne Verbindungen, VPN, STUN und TURN sind bereits berücksichtigt, jedoch ist das Vorgehen gegenüber neuen Verfahren offen. ICE als neues Protokoll zu bezeichnen wäre falsch: vielmehr setzt das Verfahren auf bestehende Protokolle auf und ergänzt diese um notwendige Parameter, namentlich handelt es sich um SDP und TURN. Mit J. Rosenberg als Autor ist ICE klar in der SIP-Welt beheimatet und dafür entwickelt worden. Jedoch wird mehrfach darauf verwiesen, dass ICE nicht nur für SIP und UDP funktioniert, sondern einen generelleren Ansatz verfolgt. (siehe Abbildung 15)

ICE beschreibt, wie eine Verbindung zwischen zwei Gesprächspartnern aufgebaut wird, wobei während des Aufbaus ermittelt wird, welche Verfahren in Frage kommen und welches davon wiederum, das günstigste ist.

Im ersten Schritt geht der Anrufer hin und sammelt alle zur Verfügung stehenden Verfahren und die dazu gehörigen IP Adressen. Im Beispiel von Abbildung 15 wären das drei Stück: direkte Kommunikation mit der eigenen IP Adresse, „geNATete" Kommunikation mit der durch STUN ermittelten externen IP Adresse und „geTURNte" Kommunikation mit der vom TURN-Server zugewiesenen IP Adresse. Nachdem er diese Verfahren und IP Adressen kennt, wird jeder Variante eine Priorität zugewiesen.

Im zweiten Schritt wird die Verbindung zum Ziel aufgebaut: wie bei SIP üblich wird zunächst ein SIP Paket zum Empfänger gesendet. Das SDP Protokoll wird durch ICE um einen neuen Parameter erweitert, der benötigt wird, um dem Gesprächsteilnehmer mitzuteilen, welche Möglichkeiten es alles gibt, welche IP Adressen dazu gehören und in welcher Reihenfolge sie priorisiert sind. Zusätzlich wird aber auch schon eine der Verbindungsmöglichkeiten als „activ" gekennzeichnet, damit ein sofortiger Verbindungsaufbau möglich ist, vorausgesetzt das aktive Verfahren ist übehaupt geeignet eine Verbindung aufzubauen.

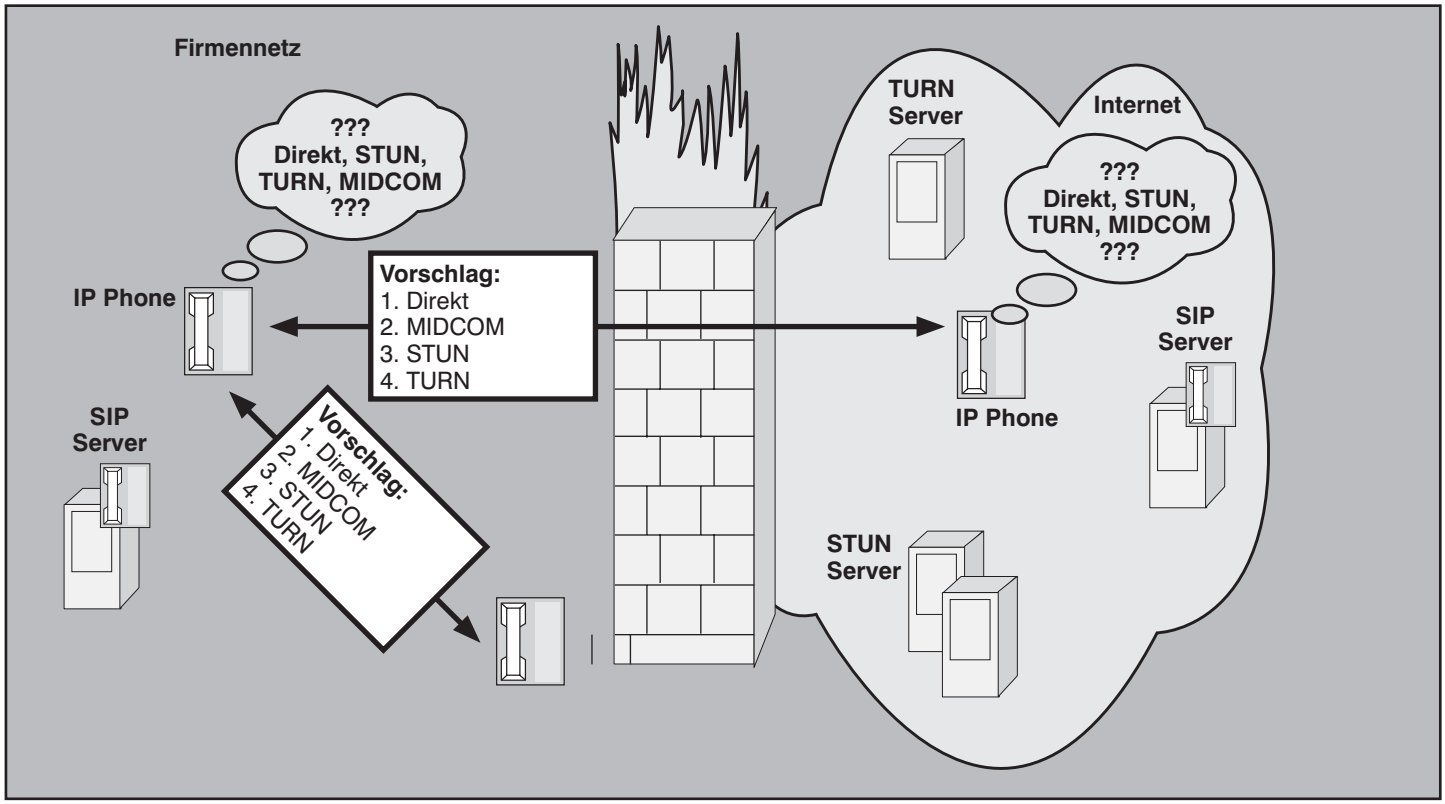


Abbildung 14: ICE Übersicht

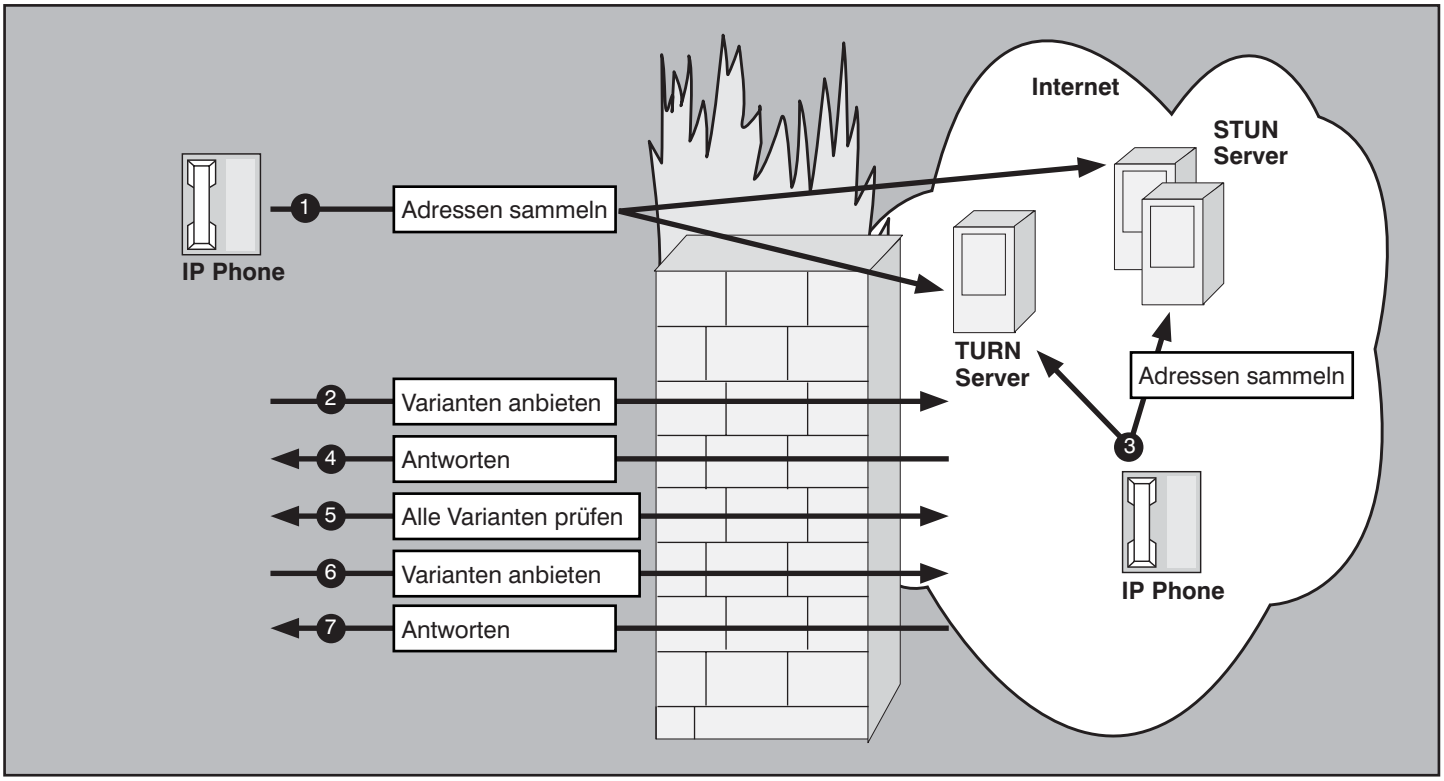


Abbildung 15: ICE Ablauf

Sobald der Empfänger den Verbindungswunsch signalisiert bekommt, kommt es zum dritten Schritt von ICE: der Empfänger sammelt, wie zuvor der Sender, alle Informationen: welche Verfahren mit welchen IP Adressen ihm zur Verfügung stehen. Priorisiert diese, wählt eine aktive Variante und sendet die Informationen mittels SDP zurück.

Im vierten Schritt wird nun getestet, ob als „aktiv" markierte Verfahren einen Verbindungsaufbau zulassen. Dazu werden STUN Pakete genutzt, die sich die Gesprächspartner zuschicken und die so parametrisiert sind, dass sie sich für den Test eignen. Ist ein Verbindungsaufbau möglich, wird gleich ein Mediastream in jede Richtung etabliert. Funktioniert mindestens eines der aktiven Verfahren nicht, so werden die anderen vorgeschlagenen Verfahren gemäß ihrer Priorität getestet, bis eines davon einen Verbindungsaufbau ermöglicht.

Nun kann es sein, dass das ursprünglich gewählte, aktive Verfahren zwar möglich aber nicht günstig ist. Beispiel: ein mobiler Mitarbeiter baut über das Internet eine VPN Verbindung in seinen Heimatstandort auf, der VPN Zugang lässt eine gleichzeitige Verbindung zum Internet zu. Dann wäre TURN (über das Internet) genauso möglich wie die „direkte" Verbindung über das VPN. Da die Firma viele Anrufe aus dem Internet bekommt, ist TURN als Default eingestellt, im Falle des mobilen Users ist VPN jedoch günstiger. In diesem Fall wird, um den Verbindungsaufbau für den User möglichst kurz zu halten, sofort über TURN eine Verbindung hergestellt, anschließend wird die Liste der angegebenen Möglichkeiten jedoch noch weiter durchgetestet, um festzustellen, ob es nicht eine bessere, höher priorisierte Lösung gibt. Bei diesem Test würde im Beispiel VPN als das bessere Verfahren herauskommen. Deswegen werden erneut SIP Pakete ausgetauscht, in denen nun VPN als aktiv markiert wird. Abschließend werden die beiden Medienstreams auf das VPN umgestellt.

Das Verfahren ist abwärtskompatibel, soll heißen, ein ICE fähiger Client kann auch mit einem nicht ICE fähigen interagieren. Der Trick ist einfach und liegt in der Art, wie SDP mit unbekannten Parametern umgeht: ein Empfänger ignoriert alle unbekannten Parameter im SDP-Teil. Sendet der Anrufer ICE Informationen, so versteht der Empfänger sie nicht. Folglich ignoriert er sie und nutzt die „aktive" Verbindung (ein „alter", notwendiger SDP Parameter). Seinerseits sendet er in seiner Antwort keine ICE Informationen. Am Fehlen der neuen Parameter erkennt der ursprüngliche Sender, dass sein Partner kein ICE versteht und lässt es selbst (auch) bleiben.

Der große Vorteil von ICE ist, dass die Restriktionen, die die anderen Verfahren mitbringen, aufgehoben werden: jetzt ist sowohl interne wie externe Kommunikation möglich, da jeder Client verschiedene IP Adressen als Empfangsadressen angeben kann. Auch können bislang unvereinbare Verfahren nun parallel betrieben werden.

Allerdings hat der ICE zum heutigen Zeitpunkt einen entscheidenden Nachteil: es existiert nur in der Theorie und dort auch noch in halbgarem Zustand: weder ist der Standard fertig noch gibt es Komponenten, die das Verfahren unterstützen. Immerhin: dieser Draft ist noch nicht totgesagt.

3.9 Welches Verfahren für welche Anwendung

Die spannende Frage ist, welche dieser vielen vorgestellten Möglichkeiten eigentlich für welchen Einsatzfall am geeignetsten ist. Insbesondere ist diese Frage auch für das ICE Verfahren entscheidend, da man dort eine Auswahl und Priorisierung trifft. (siehe Tabelle 1)

Tabelle 1 zeigt eine solche Übersicht, die generell eine Beziehung zwischen Verfahren und Einsatzzweck herstellt. Im eigenen, speziellen Fall muss natürlich eine Einzelwertung unter Berücksichtigung der Verfügbarkeit und der Kosten getroffen

	VPN	Port Forwarding	ALG	UPnP	MIDCOM	STUN	TURN	ICE	Tanberg	Ingate
Private Anwender	nein	ja, in Verbindung mit STUN	ja, in Verbindung mit STUN aber teuer	ja	unsinnig	ja, in Verbindung mit Port Forwarding oder ALG	möglich	unnötig	nein	nein
Standort zu Standort	ja	nein	unsinnig	unsinnig	unsinnig	unsinnig	möglich	ja	unsinnig	unsinnig
Mobile User zu öffentlichem Netz	nein	nein	nein	nein	nein	unsinnig	möglich	ja	ja (Softclient)	nein
Mobile User zu Standort	ja	nein	nein	nein	nein	nein	möglich	ja		
SoHo zu öffentlichem Netz	nein	ja	ja	möglich	unsinnig	ja	ja	ja	ja (Softclient)	nein
SoHo zu Standort	ja	nein	unsinnig	unsinnig	unsinnig	unsinnig	möglich	ja	ja (Softclient)	nein
Standort öffentliches Netzwerk	nein	nein	möglich in Verbindung mit STUN	unsinnig	ja	ja, in Verbindung mit ALG oder MIDCOM	ja	ja	ja	ja
Alles muss möglich sein (Firmennetz)	ja, in Verbindung mit ICE	nein	ja, in Verbinddung mit ICE	nein	ja, in Verbindung mit ICE	ja, in Verbindung mit ICE	in Verbindung mit ICE sinnvoll	ja	ja	ja

Tabelle 1: Welches Verfahren bei welchem Anwendungsfall

werden. Will man ICE einsetzen, so fehlt auch noch die Priorisierung. Jedoch kann die Tabelle als Vorlage für eine eigene Matrix dienen.

4 Propietäre Herstellerlösungen

Auch wenn die bislang vorgestellten Standards ein breites Spektrum von Lösungen des Traversal Problems von VoIP abdecken, so leiden die beiden entscheidenden, namentlich TURN und ICE, jedoch an einem großen Problem: es gibt sie in der Praxis noch nicht. Auch wenn grundsätzlich standardisierten Verfahren gegenüber propietären der Vorzug zu geben ist, werden wegen dieses Mankos im Folgenden zwei Herstellerlösungen der Firmen Tandberg und Ingate vorgestellt, die dem TURN Ansatz ähnlich sind und den Vorteil haben, bereits zu existieren.

4.1 Tandberg

Die erste Lösung, die hier vorgestellt werden soll, ist das System der Firma Tandberg - nicht zu verwechseln mit der gleichnamigen Firma, die beispielsweise Bandsicherungs-Lösungen herstellt. Die Lösungen für NAT-Traversal werden unter dem Marketing Begriff „Tandberg Expressway" zusammengefasst. (siehe Abb. 16)
Das System setzt auf zwei Komponenten: den Gatekeeper und den Border Controller. Die Idee ist dabei folgende:

Auf jeder Seite der Firewall wird eine Komponente installiert: intern der Gatekeeper und extern der Border Controller. Während der Gatekeeper internen Geräte gegenüber vorgibt, der Gesprächspartner zu sein, simuliert der Border Controller den externen Anrufern gegenüber, er wäre der gewünschte (interne) Kommunikationspartner.

Zwischen dem Gatekeeper und dem Border Controller wird für die Signalisierung eine TCP Verbindung aufgebaut. Diese TCP Verbindung hat zusätzlich den Vorteil, dass sie dafür sorgt, dass bei jedweder NAT Variante dieselbe öffentliche IP Adresse genutzt wird, da sie nach ihrem Aufbau von beiden Servern nicht abgebaut wird und so für die Kommunikation zwischen den beiden für einen ständigen Eintrag in der NAT Tabelle sorgt.

Ein Anruf läuft folgendermaßen ab: ein externes Gerät will beispielsweise über einen SIP Proxy (H.323 ist auch möglich) die Verbindung zu seinem internen Teilnehmer aufbauen.

Die internen Geräte sind im Internet mit der IP Adresse des Border Controllers registriert. Sobald der externe Client somit dem Border Controller signalisiert, dass er einen Gesprächsaufbau wünscht, gibt der Border Controller die notwendigen Informationen an den Gatekeeper weiter. Der Gatekeeper seinerseits signalisiert nun einen Gesprächsaufbau an den angerufenen Client mit denselben Verbindungsparametern, die bereits der externe Client benutzte: welche Codecs genutzt werden sollen, ob nur Sprache oder auch Video etc. Einziger, aber entscheidender Unterschied bei den Parametern: er gibt dem internen Client gegenüber vor, der Anrufer zu sein; sprich, er trägt seine eigene IP Adresse im Signalisierungsprotokoll als Absender ein.

Der interne Client beantwortet den Gesprächswunsch dem Gatekeeper, der gibt die Antwort an den Border Controller und der wiederum leitet sie an den externen Anrufer weiter, wobei er so tut, als wäre er der gewünschte Gesprächspartner, also ebenfalls ein Austausch der IP Adressen im Signalisierungsprotokoll.

Nachdem die Signalisierung abgeschlossen ist, werden die Mediastreams aufgebaut: der interne Client mit dem Gatekeeper und der externe mit dem Border Controller. Ebenso werden die Media-Daten natürlich zwischen den beiden Servern ausgetauscht. Dabei können die beiden jedoch die UDP-Portnummern so anpassen, dass sie den voreingestellten Regeln der Firewall entsprechen. Zwischen Border Controller und Gatekeeper müssen also nicht alle UDP Ports erlaubt sein, sondern man kann sich auf eine recht enge Portrange beschränken.

Beide Komponenten erinnern stark an TURN-Server, es gibt jedoch einen großen Unterschied, der zugleich die Stärke wie auch die Schwäche der Lösung von Tandberg ist: beide Komponenten sind für die Endgeräte transparent. Der Vorteil ist,

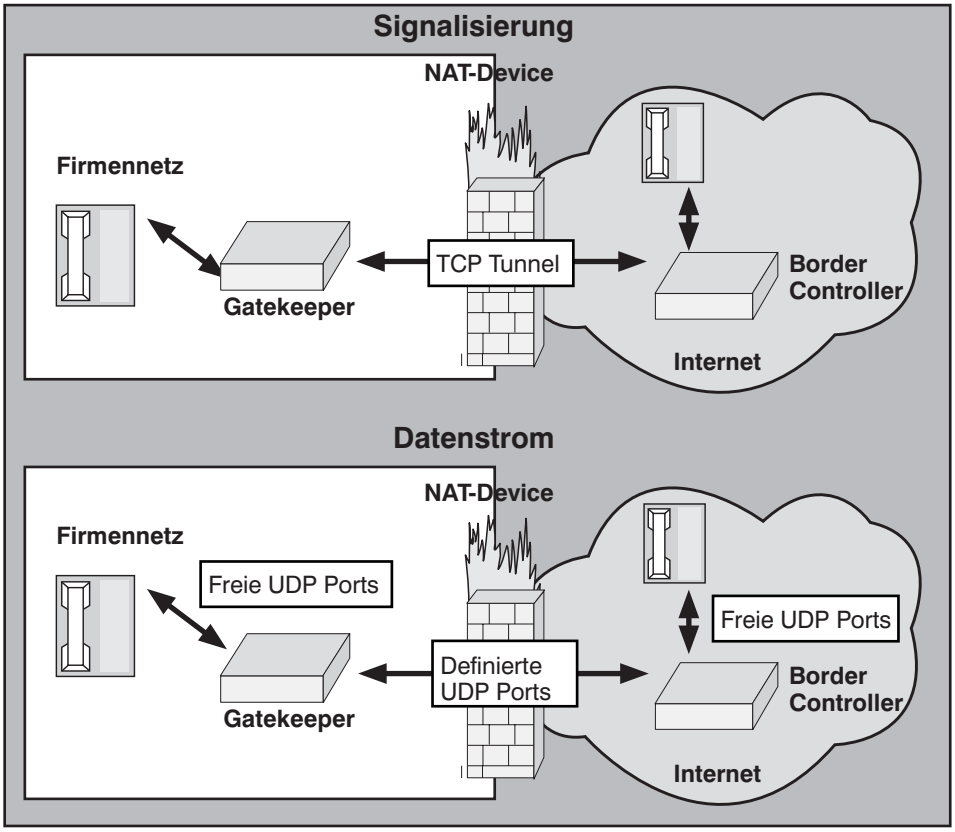


Abbildung 16: Tandberg-Lösung für die Kommunikation mit dem Internet

dass das Verfahren sofort einsetzbar ist und keine speziellen Clients benötigt werden. Der Nachteil ist jedoch, dass beide die Signalisierungsprotokolle verstehen müssen, um die notwendigen Änderungen an der Signalisierung vornehmen zu können. Damit bekommt Tandberg Probleme mit propietären Signalisierungen und u.U. auch mit Parametern, die von Herstellern ergänzt werden.

Ein weiteres Problem ist, dass durch die notwendigen Änderungen in der Signalisierung und im Relaying der Mediaströme das Ende-zu-Ende Delay erhöht wird. Was zudem einen Ressourcen-Engpass darstellen kann, ist, dass einer der Server überlastet wird. (siehe Abbildung 17)

Auf zwei Besonderheiten der Lösung soll noch kurz eingegangen werden.

Auch wenn in der Beschreibung des Verfahrens die Kommunikation zwischen einem Client im Internet und einem im internen Netz beschreiben wurde, so ist es auch geeignet, um zwei Standorte miteinander zu verbinden, wie man anhand von Abbildung 17 leicht erkennen kann.

Man kann sich sogar vorstellen, wie die Kommunikation zwischen zwei privaten Netzen aussähe, die mit eigenen Border Controllern arbeiten: Anrufer zu Gatekeeper (Firma A) zu Border Controller (Firma A) zu Border Controller (Firma B) zu Gatekeeper (Firma B) zu Angerufenem.

Wie schon zuvor bemerkt, gilt für die beiden letztgenannten Lösungen natürlich, dass sich das Ende-zu-Ende Delay deutlich erhöhen wird, das ein kritischer Parameter bei der VoIP-Kommunikation ist. (siehe Abbildung 18)

Will man auf den Gatekeeper ganz verzichten, so ist das auch möglich, indem man die von Tandberg entwickelten Softclients nutzt. Dabei handelt es sich um Video-fähige VoIP Clients, die zusätzlich die Funktion des Gatekeepers übernehmen können. Also für die Signalisierung einen eigenen TCP Tunnel zum Border Controller aufbauen und mit konfigurierbaren Ports für die Mediastreams arbeiten. Diese Variante wird in Abbildung 18 dargestellt.

Erinnerten schon die Lösung mit Gatekeeper stark an die sich in der Standardisierung befindlichen TURN Lösung, so kann man bei dieser letzten Variante mit speziellen Clients den Unterschied kaum noch erkennen. Vom Vorgehen her sind sie nahezu identisch, die Unterschiede liegen in den Details, wie Erstellen von Dial-Plänen, Registrierung an öffentlichen SIP-Re-

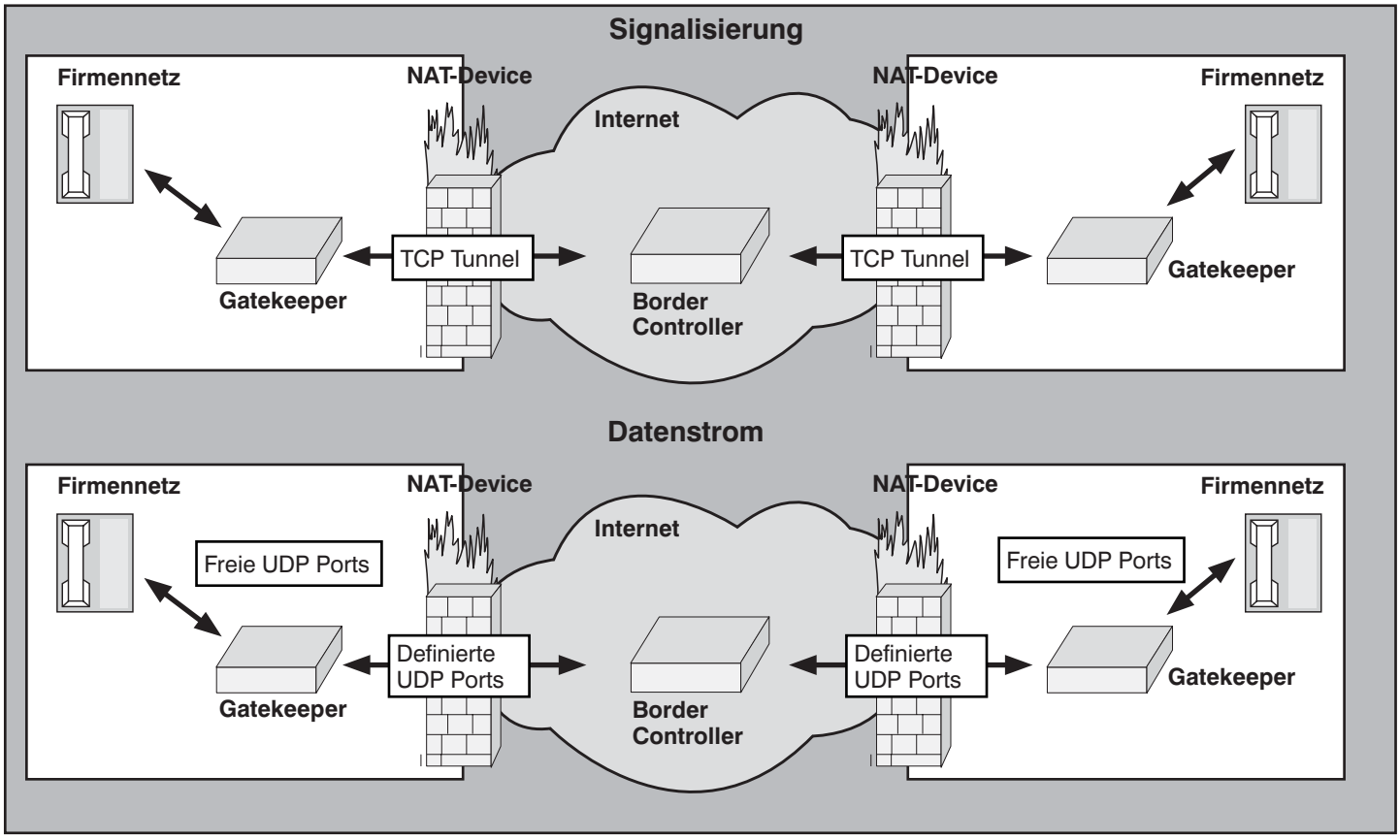


Abbildung 17: Tandberg-Lösung für die Kommunikation zweier Standorte über das Internet

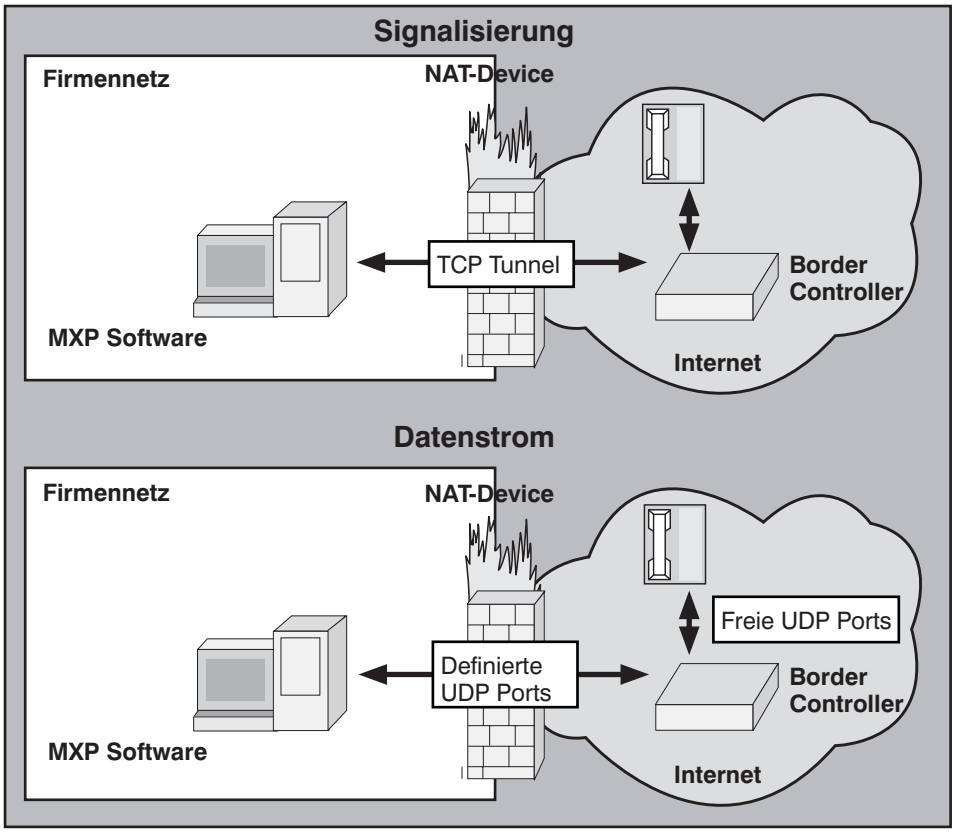


Abbildung 18: Tandberg Lösung für spezielle VoIP Clients

gistrars und der TCP Verbindung für die Signalisierung.

Abschließend noch der wohl größte Nachteil von Tandberg zum aktuellen Zeitpunkt: bislang arbeitet es nur mit H.323 Clients, nicht mit SIP, wie im Beispiel vorgestellt, doch zeichnet sich auch dafür eine Lösung am Horizont ab.

4.2 Ingate

Ist die Tandberg Lösung stand heute nur für H.323 verfügbar und nicht für SIP, so ist das bei der Ingate Variante genau umgekehrt. (siehe Abbildung 19)

Ingate kommt mit einer zusätzlichen Komponente aus, dem SIP Konzentrator. Dieser übernimmt die Rolle der SIP Server (e.g. SIP Proxy, Registrar etc.) für interne Clients. Zusätzlich - wie bei Tandberg - simuliert er dem internen Client gegenüber, der Gesprächspartner zu sein. Anders als die Tandberg Variante simuliert er aber auch dem externen Gesprächspartner, er wäre der interne Client. Der SIP Konzentrator ist also Gatekeeper und Border Controller in einem.

Damit das funktioniert, benötigt der Konzentrator selbst entweder eine öffentliche IP Adresse oder aber auf der Firewall

muss ein entsprechendes Portforwarding eingeschaltet werden, so dass die Mediastreams zu ihm geleitet werden. Damit nicht alle eintreffenden UDP Pakete an den Konzentrator gesendet werden, können auf ihm spezielle Ports konfiguriert werden, die für die Medien-Daten genutzt werden.

Der Verbindungsaufbau sieht dann wie folgt aus:

Zunächst registrieren sich die Clients an „ihrem" SIP Server, also dem Konzentrator. Dieser registriert nun die Telefonnummer der Clients an einem öffentlichen SIP Registrar, jedoch mit seiner IP Adresse (ggf. der „geNATeten"). Ruft nun ein externer Client einen internen Client an, so sendet er die Signalisierung an seinen Proxy, der gibt sie an den Konzentrator weiter, da er diesen für das Endgerät hält. Der Konzentrator seinerseits signalisiert nun dem internen Client den Anruf und handelt mit ihm die Gesprächsparameter aus, wobei dynamische Ports intern kein Problem sind. Gleichzeitig handelt er auch mit dem externen Client die Verbindungsparameter aus, dieses Mal jedoch greift der Konzentrator auf vorher festgelegte Ports zurück, die auch von der Firewall richtig weitergeleitet werden.

Ist die Signalisierung in beide Richtungen abgeschlossen, werden die Medien-Kanäle aufgebaut. Der Konzentrator relayed die Media-Pakete und führt die notwendigen Änderungen bei den Portnummern durch. (siehe Abbildung 20)

Grundsätzlich kann der SIP Konzentrator auch parallel zur Firewall betrieben werden, dazu hat er eine öffentliche und eine private IP Adresse (Abbildung 20). In diesem Fall übernimmt er zusätzlich zu den bereits beschriebenen Aufgaben auch das NAT selbst. Vorteil dieser zweiten Lösung gegenüber der internen Platzierung ist, dass die Firewall bei der SIP Kommunikation außen vor ist: somit stellt sie keine zusätzliche Fehlerquelle mehr dar und es gibt keinerlei „neue" Anforderungen, die sie erfüllen muss.

Nachteil der Ingate Lösung ist ihre Beschränktheit auf SIP. Da der Konzentrator vorgibt, Client zu sein, muss er - wie auch schon Tandberg - alle Protokoll-Parameter beherrschen, die die Clients beherrschen, um seine Aufgabe erfüllen zu können. Das kann bei propietären Erweiterungen, wie sie heute bei SIP üblich sind, so weit führen, dass die Kommunikation nicht mehr aufgebaut werden kann.

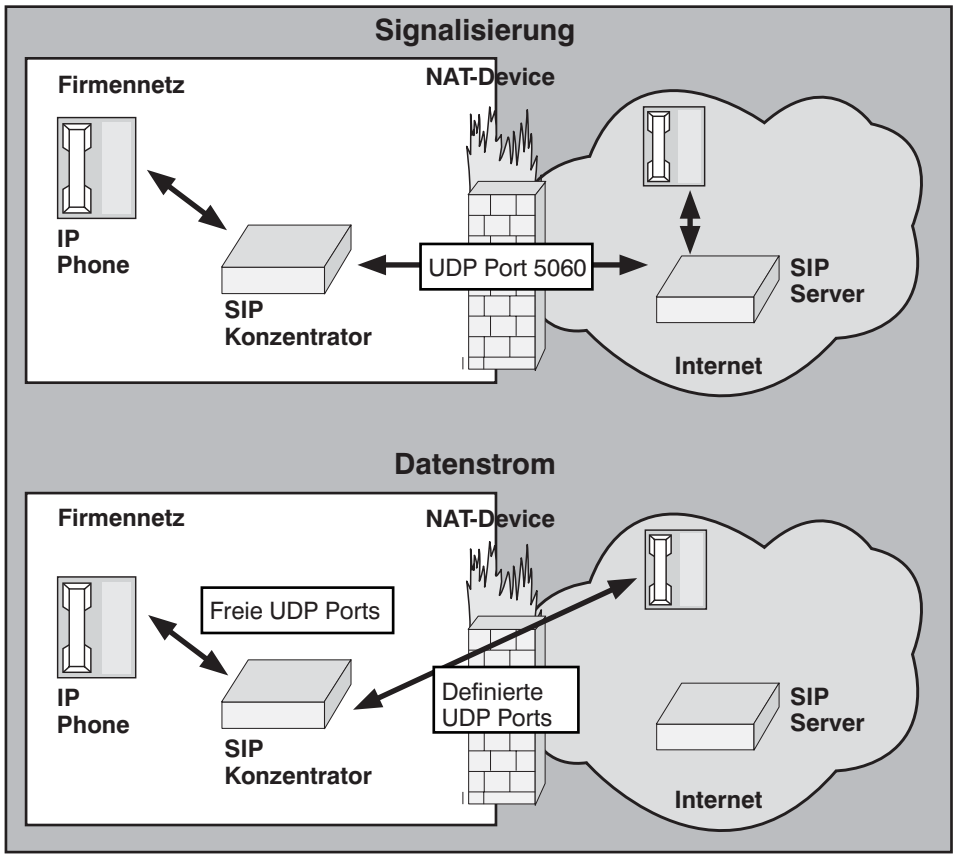


Abbildung 19: Ingate Lösung für NAT Traversal über eine Firewall

5 Bewertung

Betrachtet man alle Lösungen und Lösungsansätze, die zum Teil sehr unterschiedlich sind, so ergibt sich folgendes Bild: eine allumfassende, immer funktionierende und alle glücklich machende Lösung existiert noch nicht. Stand heute ist, dass dringend erforderliche Standards noch in den Kinderschuhen stecken und die propietären Lösungen darunter leiden, dass sie nur Teilaspekte abdecken können und versagen, wenn Erweiterungen anderer Hersteller in den Signalisierungsprotokollen zum Einsatz kommen.

Zudem existieren jedoch auch heute schon Lösungen, die einen Teil der möglichen Anforderungen abdecken (e. g. STUN + ALG). Je nach eigenem Firewall Design und eigenen Sicherheitsrichtlinien ist es somit bereits heute in einigen Fällen möglich, das Problem in den Griff zu bekommen.

Auf der anderen Seite ist das Problem aus dem Internet eintreffender VoIP-Anrufe für die meisten Unternehmen aber noch nicht aktuell, so dass man zumindest für einige Zeit noch abwarten kann, ob sich der ICE und TURN Ansatz gegenüber propietären Lösungen durchsetzt.

6 Anhang

6.1 Literaturverzeichnis

Homepage des UPnP Forums- Sammlung von Whitepapers und „Standards" - http://www.upnp.org/default.asp

Middlebox communication architecture and framework - RFC3303 - http://www.rfc-editor.org

Middlebox Communications (midcom) Protocol Requirements - RFC3304 - http://www.rfc-editor.org

Middlebox Communications (MIDCOM) Protocol Semantics - RFC3989 - http://www.rfc-editor.org

Middlebox Communications (MIDCOM) Protocol Evaluation - RFC4097 - http://www.rfc-editor.org

Simple Traversal of User Datagramm Protocol (UDP) Through Network Address Tranlators (NATs) - RFC3489 - http://www.rfc-editor.org

Studie zur Sicherheit von Voice over Internet Protocol BSI: VoIPSEC - http://www.bsi.de/literat/studien/VoIP/

Interactive Connectivity Establishment (ICE) - draft-ietf-mmusic-ice-06 - http://www.rfc-editor.org

Traversal Using Relay NAT (TURN) - draft-rosenberg-midcom-turn-08 - http://www.rfc-editor.org

Übersicht über die Tandberg Lösungen - Sammlung von Whitepapers - http://www.tandberg.net/products/tandberg_expressway.jsp

Homepage von Ingate - http://www.ingate.com/

6.2 Abkürzungen

ALG	Application Layer Gateway, auch Application Level Gateway
B2B	Business to Business
COPS	Common Open Policy Service
Diameter	potentieller Nachfolger von RADIUS
ICE	Interactive Connectivity Establishment
IP	Internet Protocol
Megaco	Media Gateway Control Protocol
MIDCOM	Middlebox Communication
NAPT	Network and Port Address Translation
NAT	Network Address Translation
PAT	Port Address Tranlation
RADIUS	Remote Access Dial-In User Service
RSIP	Realm Specific IP
RTP	Real Time Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protcol
SNMP	Simple Network Management Protocol
STUN	Simple Traversal of User Datagramm Protocol (UDP) Through Network Address Tranlators (NATs)
TURN	Traversal Using Relay NAT
UDP	User Datagramm Protocol
UPnP	Universal Plug and Play
VPN	Virtual Private Network

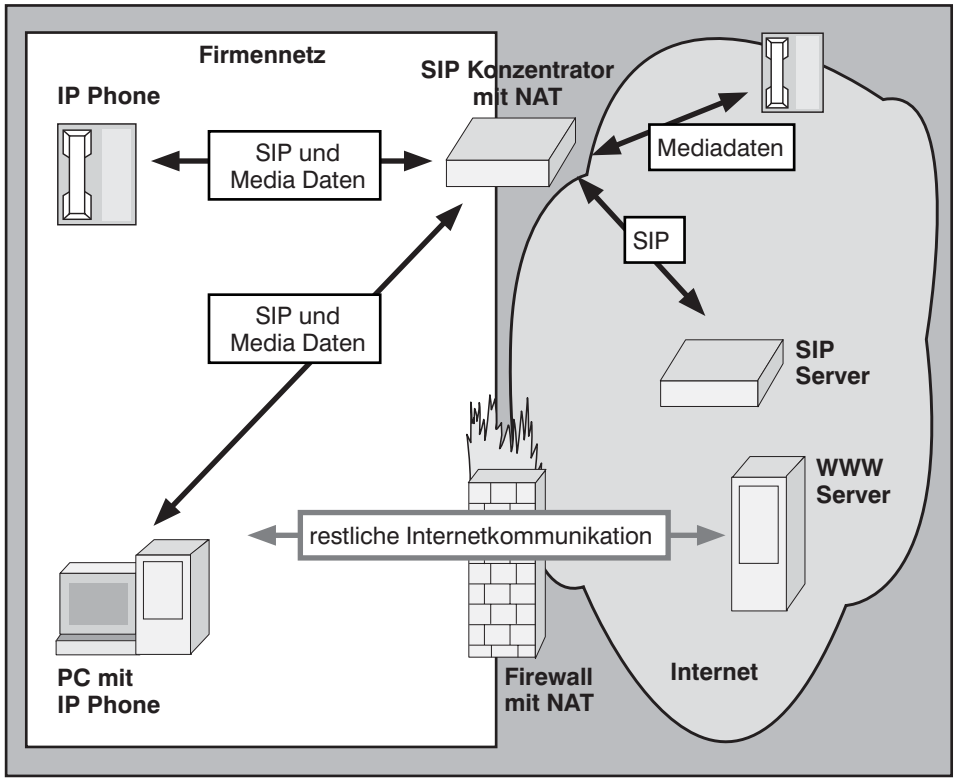


Abbildung 20: Ingate-Lösung mit spezieller SIP-Firewall

CCNE

ComConsult Certified Network Engineer

Lokale Netze
28.11. - 02.12.05 in Aachen
06.02. - 10.02.06 in Aachen
03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

Internetworking
28.11. - 02.12.05 in Aachen
06.03. - 10.03.06 in Aachen
08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP
14.11. - 18.11.05 in Bonn
13.02. - 17.02.06 in Bonn
15.05. - 19.05.06 in Stuttgart
25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand
20.02. - 24.02.06 in Aachen
29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

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

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
20.03. - 24.03.06 in Aachen
08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
28.11. - 02.12.05 in Aachen
27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
30.01. - 03.02.06 in Aachen
24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 in Aachen

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

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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung
06.02. - 10.02.06 in Köln
15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
20.03. - 22.03.06 in Bad Neuenahr
19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
05.12. - 09.12.05 in Aachen
03.04. - 07.04.06 in Aachen
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

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

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

Impressum

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

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

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