Dr. Suppan International Institute

Der Netzwerk Insider

Mai 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

von Dipl.-Inform. Petra Borowka

Jahrelang war die H.323-Suite der ITU-T die Standard-Basis für IP Telefonie. Nun gibt es eine breite Welle von SIP-Ankündigungen und Verfügbarkeiten bei Herstellern und Carriern. Wird SIP H.323 verdrängen? Wo liegen die Vorteile? Wo die Grenzen? Ist SIP eine Technik, die proprietären Signalisierungen der etablierten Enterprise VoIP Lösungen Konkurrenz macht? Der nachfolgende Beitrag gibt eine Beschreibung der Technik und eine Bewertung der Marktrelevanz von SIP und den zugehörigen Standards.

Dieser Beitrag setzt ein grundsätzliches Verständnis voraus, wie IP Telefonie funktioniert und welche Basis-Protokolle und Verfahren hier zum Einsatz kommen. Für eine Einführung in Voice over IP verweisen wir auf die Netzwerk Insider vom September und November 2000. (Bei Bedarf können Sie diese per E-Mail unter: **info@comconsult-akademie.de** anfordern)

weiter auf Seite 14

Zweitthema

Neues bei TCP/IP?!

von Dipl.-Inform. Oliver Flüs

Gibt es überhaupt Bedarf zur Beschäftigung mit „Neuerungen“?

Neues bei TCP/IP, das hört sich für manche so spannend an wie „Opa hat neue Zähne“ und für andere wie „wer keine Probleme hat, der sucht sich welche“: Warum nach Neuigkeiten im Bereich TCP/IP Ausschau halten, es läuft doch alles rund?

Damit ist es aber nicht getan! „Netzwerke leben“, und bei stabiler, relativ neuer Netzwerk-Technik kommt der Drang zu Veränderungen umso stärker von der Anwendungsseite her. Voraussetzung ist allerdings eine ebenso stabile wie entwicklungsfähige Basis - und das ist TCP/IP nicht zuletzt dank der praxisnahen, pragmatischen Art und Weise, wie die entsprechenden Neuerungen und Standards zustande kommen.

Das Netzwerk „lebt“ und verändert sich – und TCP/IP mit ihm

Mit TCP/IP ist es wie mit robusten Pflanzen: Aus scheinbar toten Zweigen kommt unversehens wieder Grünes hervor, und oben wachsen neue Zweige nach.

So kommt es, dass man sich auch als „gestandener Netzwerker“ regelmäßig mit Neuigkeiten rund um TCP/IP beschäftigen sollte. Eine Menge „tote Zweige“ haben in der jüngsten Vergangenheit nicht nur wieder kleine grüne Blättchen an den Tag gelegt, sondern stehen kräftig in Blüte: kaum jemand, der heute noch ein Netzwerk ohne DHCP betreibt, obwohl der Standard lange Zeit in der IETF-Bibliothek der Vorschläge vor sich hin geschlafen hat.

weiter auf Seite 6

Top-Event

ComConsult Sommerschule 2004

auf Seite 4

Zum Geleit

Die Zukunft der Telefonie

auf Seite 2

Report des Monats

Ethernet in Industrie-Umgebungen

auf Seite 12

Zum Geleit

Die Zukunft der Telefonie

Wie entwickelt sich die TK-Welt, wie sicher sind Investitionen in traditionelles TK-Equipment, wie sicher sind Investitionen in IP-Telefonie, wie sieht die Zukunft der heutigen Anbieter aus?

Diese Fragen wurden auf dem gerade abgelaufenen Netzwerk-Redesign-Forum intensiv diskutiert. Führende Hersteller zeigten ihre aktuellsten Produktvarianten (Alcatel, Avaya, Cisco, Siemens) und stellten sich der Diskussion mit den Teilnehmern.

ComConsult-Research vertrat dabei unter dem Eindruck der zurzeit laufenden Analyse-Arbeiten einige sehr provokante Thesen:

These 1

Die Zeit herstellerspezifischer Signalisierung nähert sich dem Ende. In den nächsten 5 Jahren wird der Umbruch zu offener, standardisierter Signalisierung auf Basis von SIP erfolgen.

These 2

Die traditionellen TK-Anlagen werden vollständig durch Soft-PBX-System verdrängt werden. Maximal im Bereich von Gateways zu analogen oder bestehenden digitalen Endsystemen und zum PSTN wird Spezialhardware zum Einsatz kommen.

These 3

Die zukünftige Signalisierung wird auf dem Session Initiation Protocol SIP basieren, sich aber nicht auf reine Telefonie-Anwendungen beschränken. Allerdings werden die Hersteller voraussichtlich hingehen und die SIP-Basis-Funktionalität um herstellerspezifische Elemente erweitern.

These 4

Die Standard-PBX der Zukunft wird ein OpenSource SIP-Registrar/Proxy/Location Server sein, der auf gängiger Hardware eingesetzt werden kann. Abgespeckte Versionen von Linux werden dafür den Systemrahmen stellen (in der Konfiguration vergleichbar mit der heutigen Auslegung von gehärteten Apache-Servern). Auch Microsoft wird dieses Standbein ausbauen und für eine erhöhte Präsenz von Windows-basierten Lösungen sorgen.

These 5

Herstellerspezifisch werden Produkte sein, die die SIP-Architektur um spezielle Merkmale zur Erhöhung der Verfügbarkeit oder der Leistungsmerkmale ergänzen werden (Cluster-Bildung, Mehrstandort-Konzepte mit Failover)

These 6

Mit SIP entsteht eine neue Art der Kommunikation, die Sprache, Video und Kollaboration vereinen wird. Insbesondere wird die Kommunikation innerhalb von Teams im Rahmen von auch Standort-übergreifenden Geschäftsprozessen unterstützt werden.

These 7

Die Alleinstellungsmerkmale der Hersteller werden sich neben der Architektur stark in den Bereich der Software-Zusatz-Funktionalität und von Spezial-Applikationen verschieben. Typisch werden sein: ACD, Unified Messaging, Präsenz-Kommunikation und eben Kollaboration (Dokumenten-Sharing, Whiteboard, Messenger-Dienste)

Einen starken Einfluss auf die Weiterentwicklung und Marktbedeutung von SIP wird der Konsumer-Markt haben. Hier werden bis Ende 2005 massive Angebote der verschiedenen Provider den Konsumenten durch attraktive Preise in diese Richtung bewegen. Damit wird schnell ein relativ großer Markt für SIP-Endgeräte entstehen. Dieser wird auch das Preisgefüge im Unternehmensbereich nachhaltig verändern. Auch SIP-Clients mit erweiterten Zusatzfunktionen (Anrufbeantworter etc, siehe SIPPS-Softphone) werden sich schnell verbreiten. Die typischen SOHO-Broadband-Router/Firewall werden SIP-Proxies oder Application Level Gateways enthalten, um das NAT-Traversal-Problem zu lösen (siehe Ingate oder Intertex).

Der heute schon starke Markt für SIP-Software wird sich durch diese Entwicklung explosionsartig ausweiten. Dabei werden zunehmend OpenSource-Produkte an Bedeutung gewinnen. Auch im Konsumer-Bereich wird Telefonie dabei zunehmend um weitere Funktionen ergänzt werden.

Im Unternehmensbereich werden die traditionellen Anbieter durch diese Entwicklung immer stärker unter Druck kommen. Der Hauptgrund für den Einsatz traditioneller TK-Produkte wird sich immer stärker auf den Aspekt der Migration in die neue Welt und die damit verbundene Einbindung der vorhandenen, traditionellen Endgeräte im Sinne einer Übergangslösung beziehen.

Diese Entwicklung wird bei mittelständischen und großen Unternehmen unterschiedlich verlaufen. Zuerst wird der Mittelstand in diese neue Situation einsteigen. Im unteren Anlagenbereich werden dabei komfortable Lösungen entstehen, die mit traditioneller Technik für den Mittelstand zu teuer waren. Durch diese Entwicklung geraten die Hersteller zunehmend unter Druck, da auf der einen Seite die Konsumer und die kleineren Unternehmen das dominante Mengengerüst realisieren und immer wenige große Kunden kaum noch in der Lage sein werden, hohe Entwicklungskosten in traditionelle Lösungen zu kompensieren. Der Highend-Markt der großen Konzerne läuft so in Gefahr, für die Hersteller unwirtschaftlich zu werden. Der Wechsel auf offene TK-Technik ist damit auch in diesem Markt nur eine Frage der Zeit.

Ein Teilnehmer des Netzwerk-Redesign-Forums stellte in diesem Zusammenhang die provokante Frage, ob dies der endgültige Untergang von Siemens und der Marktgewinn von Cisco sein wird. Analysiert man die zuvor genannten Thesen, dann kommt man bezüglich dieser Frage zu einem überraschenden Ergebnis. Zwar ist Siemens durch den Rückgang der klas-

sischen TK in dem Sinne stark betroffen, dass wesentliche Umsatzträger verschwinden werden. Trotzdem ist Siemens auf die zu erwartende Umstellung nicht schlecht vorbereitet. So arbeitet man seit Jahren an einer Verstärkung der Software-Angebote im Bereich TK. Nur wenige Hersteller außer Siemens verfügen über ein so breites Angebot an Zusatzsoftware. Parallel hat Siemens mit dem OpenScape-Ansatz den Einstieg in eine neue Form der Telefonie begonnen, der komplett auf der Linie der in Zukunft zu erwartenden Produkte liegt. Lediglich die Bindung an Microsoft wirkt bei diesem Ansatz stark diskussionswürdig. Ein neutraler SIP-Server mit entsprechenden Messenger-Funktionalitäten wäre eine interessante Alternative.

Betrachtet man die Situation von Cisco, dann ist die Lage nicht so positiv wie auf den ersten Blick zu erwarten. Cisco wird mit dem Wechsel auf SIP seine herstellerspezifische Signalisierung aufgeben müssen. Die heutigen, relativ teuren Endgeräte werden von preiswerten Massenprodukten bedrängt werden. Die Stärke von Cisco ist in der Basis-Architektur zu sehen. Die Schwäche von Cisco ist die Abhängigkeit von externer Software. Im Gegensatz zu Siemens hat Cisco bewusst auf eine starke Software-Entwicklung verzichtet und auf Partner gesetzt. Auch wenn dies funktional zu befriedigenden Ergebnissen führen kann, so besteht doch im Sinne der beschriebenen Zukunfts-Perspektiven der erhebliche Nachteil, dass genau mit dieser Software in Zukunft das Geld verdient werden wird. Cisco hat so auf den eigentlichen in Zukunft zu erwartenden Mehrwert verzichtet.

Im Ergebnis sind also Cisco und Siemens von dieser Entwicklung stark betroffen. Alcatel und Avaya haben früher angefangen, auf diese Situation zu reagieren. Auch Nortel zeigt aktuell starke Tendenzen in die neue Richtung. In Summe wird diese Entwicklung aber für den gesamten Markt mit erheblichen Umbrüchen verbunden sein. Immerhin hängen an der Entwicklung, dem Vertrieb und der Wartung der traditionellen TK-Anlagen viele Arbeitsplätze und komplexe logistische Strukturen. Diese Strukturen werden sich stark ändern, wenn nicht sogar komplett zerschlagen werden. Software-Entwicklung wird immer stärker aus Deutschland verlagert, der gesamte Bereich der heutigen Produktion wird somit in Zukunft bei Software-Entwicklern im Ausland liegen. Da Software-Entwicklung wesentlich beweglicher ist als eine Fabrik, die materielle Güter produziert, können die großen Hersteller damit ihre Kosten und ihre Standort-Flexibilität erheblich optimieren.

In der Software liegt die Zukunft der Telekommunikation. Dies ist mein bisheriges Zwischenfazit aus den Arbeiten der letzten Monate. Unklar ist im Moment, wie schnell diese Entwicklung stattfinden wird. Wie schon ausgeführt, wird der Konsumer-Markt auf diesen Zeitverlauf einen deutlichen Einfluss haben.

Besteht somit das Risiko einer Fehlinvestition, wenn heute noch in traditionelle TK-Technik oder eine IP-basierte herstellerspezifische Lösung investiert wird? Diese Frage kann nicht pauschal beantwortet werden. Zum einen sind offene Produkte in der notwendigen Ausprägung noch nicht ausreichend verfügbar. Zum anderen wird je nach bestehender Installationsbasis ein individuell optimierter Weg in die Zukunft entwickelt werden müssen.

Entscheidend ist aber auch, was ein Unternehmen eigentlich unter Kommunikation versteht. Reduziert sich das auf Sprachkommunikation im traditionellen Sinne, dann gibt es nur einen geringen Handlungsdruck. Hier kann das Verlängern bestehender Verträge und das geduldige Abwarten der Marktentwicklung in Richtung offener Lösungen sogar die sinnvollste Alternative sein.

Hat ein Unternehmen allerdings einen weitergehenden Kommunikationsbegriff, dann kann eine umgehende Investition in neue Technologien sehr sinnvoll sein. Zwei typische Funktionsbereiche sollen an dieser Stelle genannt werden:

1) Einbindung mobiler Mitarbeiter: wie können mobile Mitarbeiter egal an welchem Ort sie sich befinden optimal in die Arbeitsabläufe des Unternehmens integriert werden.

2) Zusammenarbeit in Standort-übergreifenden, ggf. international verteilten Teams. Ein Kernthema der zunehmenden Globalisierung. Das immer aktueller werden Schlagwort ist Kollaboration.

Analysiert man diese beiden Beispiele, dann wird die damit verbundene Komplexität sofort klar. Kollaboration entsteht ja nicht dadurch, dass ein SIP-Client Dokumenten- oder Application-Sharing anbietet (dies ist ein deutlich erkennbarer Trend auf der Produktseite, siehe als Beispiel Session von WaveThree). Wer in verteilten Teams gemeinsam an Dokumenten arbeiten möchte, muss vorher Abläufe formalisieren und umfangreiche Standardisierungen vornehmen: einheitliche und versionsidentische Applikationen und Datenformate (Textverarbeitung, Tabellenkalkulation, Grafik, Datenbank, Web, …), einheitliche Verzeichnisstrukturen, Format des gespeicherten Dokuments, eingesetzte Schrifttypen, eingesetzte Formatvorlagen, eingesetzte Grafik-Lösung bis hin zu einheitlichen Icons. Damit nicht genug. Wird zudem ein Änderungs-Management von Dokumenten genutzt mit Kommentar-Management und Konsolidierung verschiedener Versionen (siehe Kampf zwischen Adobe und Microsoft um diesen Markt), muss die Nutzung dieses Versions- und Änderungs-Managements zuvor im Team klar geregelt worden sein. Trotz dieses hohen Aufwands entstehen durch standortübergreifende Kollaboration erhebliche Effizienzsteigerungen für Geschäftsprozesse, so dass dieser Aufwand in der Regel wirtschaftlich ist. Es ist aber eben zu erkennen, dass Kollaborations-Lösungen nicht durch Kauf einer Software entstehen.

Wir sind ohne Frage auf dem Weg in eine andere, wesentlich effizientere und vor allem standortneutrale Form der Kommunikation. Jederzeit an jedem Ort an allen wichtigen Geschäftsprozessen mitarbeiten können, das ist die Messlatte der Zukunft. Auf diesem Weg werden die traditionellen TK-Lösungen zunehmend unter Druck geraten.

Aber: wie das bei einem Weg so ist, sollte vor dem Beschreiten des Wegs das Ziel geklärt sein. Offene TK-Lösungen auf Basis SIP setzen einen technischen Rahmen, lösen aber keine Organsationsaufgaben. Moderne Kommunikations-Lösungen brauchen zuerst ein Konzept und dann die technische Umsetzung.

Ihr
Dr. Jürgen Suppan

Top-Event

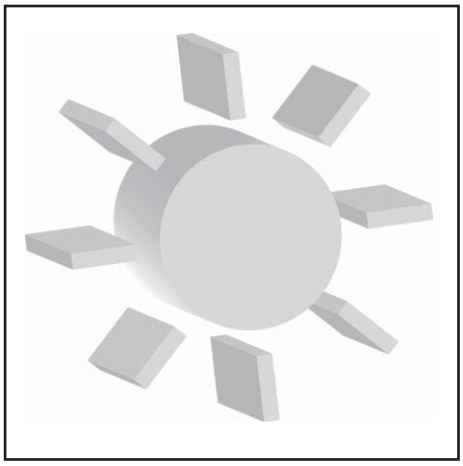
ComConsult Sommerschule 2004

Voice-over-IP-Intensiv-Evaluierung und IP Betriebsgrundlagen

Der Wechsel von der traditionellen TK zur IP-basierten TK ist in vollem Gange. Mit der HiPath 4000 Version 2 hat auch Siemens als letzter der international führenden Hersteller den Weg in die IP-Zukunft eingeschlagen. Zwar gibt es in den Projekten erhebliche Unterschiede in der Art der Migration und der Nutzung der bestehenden TK-Welt, doch der generelle Trend zur Ablösung der bisherigen TK ist nicht mehr umzukehren. Die Zahl der Projekte, in denen die IP-basierte Lösung auch in der Kostenbetrachtung für Invest und Betrieb klar vorne liegt, wird immer größer.

Die Sommerschule 2004 der ComConsult Akademie bringt Ihnen die 5-Tage-Intensiv-Evaluierung:

- wo steht VoIP heute, welche wesentlichen Entwicklungen sind noch zu erwarten?
- welche Vorteile entstehen wann und für wen?
- was leistet die aktuelle Standardisierung? Ist das Ende der Hersteller-spezifischen Lösungen nahe? Was beinhaltet der SIP-Standard, der sich immer mehr durchsetzt
- welche Anlagenarchitektur ist die beste? Hybrid oder reine Soft-PBX? Wie sind



die Redundanz-Konzepte der Anbieter zu bewerten? Für welches Einsatzszenario von der einfachen TK-Anlage über ein Filialszenario bis zur Standort-übergreifenden Lösung ist welche Architektur zu empfehlen?

- welche Sicherheits-Features sind heute realisierbar, was leisten die gerade angekündigten Sicherheits-Lösungen der Hersteller?
- was bieten die großen Hersteller, wo steht der Markt? Wie sind die aktuellen Produktlinien zu bewerten? Wer hat die Nase vorne?
- wo stehen die Haupt-Kontrahenten: Alcatel, Cisco und Siemens? Wer hat die bessere TK-Lösung für wen?
- wie entwickeln sich Preise und Leistungen, sind weitere dramatische Preis-Veränderungen zu erwarten?
- welche Anforderungen sind an den IP-Betrieb zu stellen? Welche Änderungen sind im vorhandenen IP-Management erforderlich?
- wie harmoniert IP-Telefonie mit bestehenden Sicherheits-Einrichtungen? Was ist bei der Kommunikation über eine Firewall hinweg zu beachten?
- welche Rolle spielt IEEE 802.1X in diesem Zusammenhang? Ist 802.1X überhaupt praxisreif, wie sind die Einsatzerfahrungen?
- was ist bei der Überwachung einer VoIP-Lösung zu beachten?
- welche Anforderungen gelten für ein Voice-geeignetes Netzwerk? Welche Änderungen sind erforderlich, was kosten diese? Ist der Einsatz von QoS notwendig, wie geht man damit um, wenn er nur teilweise notwendig ist?

Auf der Basis einer aktuellen Untersuchung beleuchten wir insbesondere die Marktposition, Lösungsansätze und Funktionalität zweier Marktführer in Deutschland: Cisco versus Siemens

- Leistungsmerkmale
- Architektur
- Sicherheits-Lösung
- Kosten-Bewertung
- Strategische Bewertung

12% Frühbucherrabatt bis 31.05.04

Sommerschule 2004

5 Tage Intensiv-Evaluierung zum Preis von € 2.015,-- zzgl. MwSt. statt regulär € 2.290,-- zzgl. MwSt.
Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sommerschule 2004

☐ Ich buche das Seminar
Sommerschule 2004
vom 05.07. - 09.07.04 in Aachen
(Preis € 2.015,-- zzgl. MwSt.)

*Frühbucherphase gültig bis 31.05.04.
Die Teilnahmegebühren werden mit Auslauf der Frühbucherphase fällig.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

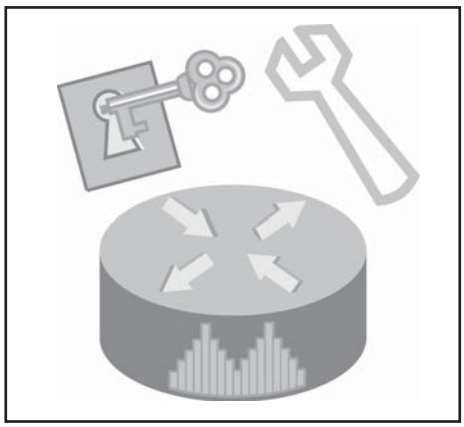
Neues Seminar

Sicherheits-Lösungen mit Cisco-Produkten

Vom 19. bis 23. Juli 2004 veranstaltet die ComConsult Akademie erstmalig ihr neues Seminar „Sicherheits-Lösungen mit Cisco-Produkten“ im Technologiezentrum der AGIT in Aachen. Dies ist das dritte Seminar unserer Cisco-Reihe.

Sicherheit wird immer wichtiger und ist so auch zu einem der beherrschenden Themen in der IT Branche geworden. Der Perimeterrouter und die Firewall am Netzzugang bilden den ersten und somit wichtigsten Schutzwall gegenüber dem Internet vor unerlaubtem Eindringen in das Firmennetz, aber sie stellen auch Technologien zur sicheren Übertragung vertraulicher Daten über das Internet zur Verfügung. Die Bandbreite der Funktionalität reicht von verschlüsselnden VPN-Techniken mit Zugangsauthentifizierungen bis zur Überwachung grundsätzlich erlaubter Kommunikationsabläufe.

In diesem Seminar lernen die Teilnehmer in Theorie und Praxis, wie man mit Hilfe von Cisco Produkten ein Firmennetz gegen unerlaubte Zugriffe absichern kann und eine sichere Verbindung zwischen Standorten und mobilen Usern herstellt. Die Theorie wird von praktischen Übungen begleitet.



Dieses Seminar ist Bestandteil unserer Cisco-Reihe und ist abgestimmt auf unsere Seminare „Cisco Router erfolgreich einsetzen - für Einsteiger“ und „Cisco Router erfolgreich einsetzen - für Fortgeschrittene“.

Profitieren Sie von unseren Paket-Angeboten und sparen Sie bis zu 10%:

Bei Buchung von zwei Cisco-Seminaren: 4.660,- € zzgl. MwSt. statt Summe der Ezelpreise 5.180,- € zzgl. MwSt. Bei Buchung von drei Cisco-Seminaren: Paketpreis 6.837,- € zzgl. MwSt. statt Summe der Einzelpreise 7.770,- € zzgl. MwSt.

In diesem Seminar lernen Sie

- Wie Sie Ihre bestehenden Cisco-Router sinnvoll zur Umsetzung von Sicherheits-Lösung benutzen können
- Welche Verfahren davon betroffen sind
- Wie diese optimal konfiguriert werden
- Mit welchem Aufwand derartige Lösungen verbunden sind

Der Referent

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 und von Cisco CCNP™ zertifiziert. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.
Markus Schaub ist ebenfalls der Referent für die Seminare „Cisco Router erfolgreich einsetzen - für Einsteiger“ und „Cisco Router erfolgreich einsetzen - für Fortgeschrittene“.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sicherheits-Lösungen mit Cisco-Produkten

☐ Ich buche das Seminar
Sicherheits-Lösungen mit Cisco-Produkten
vom 19.07. - 23.07.04 in Aachen
(Preis € 2.590,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Zweitthema

Neues bei TCP/IP?!

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von Lokalen Netzen. Im Team der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

Auch das IP-Routing hat Verbalattacken wie „Router sind lahme Kisten“ längst überstanden und stellt auf Basis moderner Layer 3-Switches mit OSPF sogar die typische Lösung für „schnelle“ Redundanzen in LAN-Backbones dar.

DDNS-Provider

Kennen Sie das Problem, dass Sie einen Webserver, Newsserver o.ä. auf Ihrem PC laufen haben, aber keine Standleitung, bzw. feste IP-Adresse besitzen, und Ihr Server trotzdem immer unter einer bestimmten Adresse erreichbar sein soll, wenn Sie online sind? Hier finden Sie eine Liste von Anbietern, die Ihnen das ermöglichen.

Diese Services funktionieren folgendermaßen:
Beim Einrichten ihres Accounts wählen Sie einen Namen aus, unter dem Sie später (in Form von „name.dienst.tld“) erreichbar Sein werden.
Wenn Sie sich einloggen übermittelt eine Software, die auf Ihrem PC läft Ihre aktuelle IP-Adresse an den Dienst, den sie benutzen. Nach ein paar Minuten (bis die neue IP-Adresse auf allen Nameservern bekannt ist, vergehen ein paar Minunten) sind Sie unter ihrer Subdomain zu erreichen.
Wenn Sie sich ausloggen, wird die IP-Adresse wieder gelöscht und es wird (jedenfalls bei manchen der Anbieter) eine von ihnen bestimmte Seite angezeigt, die aussagt, dass sie offline sind.

Abbildung 1: Dienstbeschreibung unter www.netzadmin.org/ddns-provider.php

Beispiel DDNS – mehr als nur ein bisschen „Dynamik-Option“

Auch DNS als Namensdienst, lange Zeit auf Internet und UNIX-Umgebungen beschränkt, macht nunmehr endgültig das Rennen. Mit dem Active Directory hat Microsoft seinen proprietären NetBIOS Name Service (typisch unter „WINS“ bekannt) zum Auslaufmodell erklärt, und will nunmehr konsequent auf originäre („native“) IP-Dienste aufsetzen. „Der“ Namensdienst in IP-Netzen ist aber nun mal DNS. DNS hat allerdings den Nachteil, von Hause aus statisch zu sein, handelt es sich doch von der Idee her um eine auf einen Nameserver verlagerte „Hosts-Datei für alle“. Die auf NetBIOS basierenden Windows-Mechanismen arbeiten aber mit einer dynamischen Namensverwaltung nach dem Motto, wenn ein Dienst hochfährt, wird er registriert und mit der dem Basisrechner zugehörigen IP-Adresse im Name-Service eingetragen. Also muss eine dynamische DNS-Variante her, das „Dynamic DNS“.

Wieder einmal ist das PC-Netz und damit das weit verbreitete „Windows-Netzwerk“ eine wesentliche Triebkraft, die einer guten RFC-Idee in die Fläche hilft, so wie vormals bei DHCP. Gar so neu ist DDNS schließlich nicht, der zugehörige RFC 2136 stammt aus April 1997, ist also immerhin auch schon 7 Jahre alt. Dabei ist die Ablösung von NetBIOS nicht der einzige Anwendungsfall für dynamisches „Einbuchen“ von DNS-Einträgen. Es werden dynamische DNS-updates für bestimmte Situationen als Dienstleistung im Internet angeboten.

Spätestens jetzt müssten die Alarmglocken schrillen - ein dynamischer Dienst im Internet, und auch noch einer, der die Identität von Dienstangeboten verwaltet?! Da schlummert doch ein gefundenes Fressen für irgendwelche fehlgeleitete Zeitgenossen, die nach Angriffsmöglichkeiten suchen, etwa: dem DDNS-Server die eigene IP-Adresse für ein fremdes Dienstangebot unterschieben, um dann unter fremder Identität Schaden anzurichten. So befassen sich gleich mehrere neuere RFCs mit dem Thema (D)DNS und Security, etwa RFC 3007 „Secure Domain Name System (DNS) Dynamic Update” und RFC 3008 “Domain Name System Security (DNSSEC) Signing Authority”.

Selbst bei „einfachen“ Steuerungen gibt es mindestens ein „Lernthema“: Security!

Da sind also die ersten Hausaufgaben für den IT-Betreiber im Zusammenhang mit bekannten TCP/IP-Themen - was ergibt sich aus der Themenkombination DDNS und Security? Neben den Hersteller-unabhängigen Ansätzen in RFC-Form gilt es hierbei wie so oft, auch die Produktspezialitäten zu kennen. Wie bettet sich DDNS in das Active Directory ein, was gibt es im Detail zu beachten? Was können Gründe sein, dass ein dynamisches update fehlschlägt, wie prüft man? Diese Fragen sind relevant für das Trouble Shooting, und offensichtlich auch schon so häufig bei der

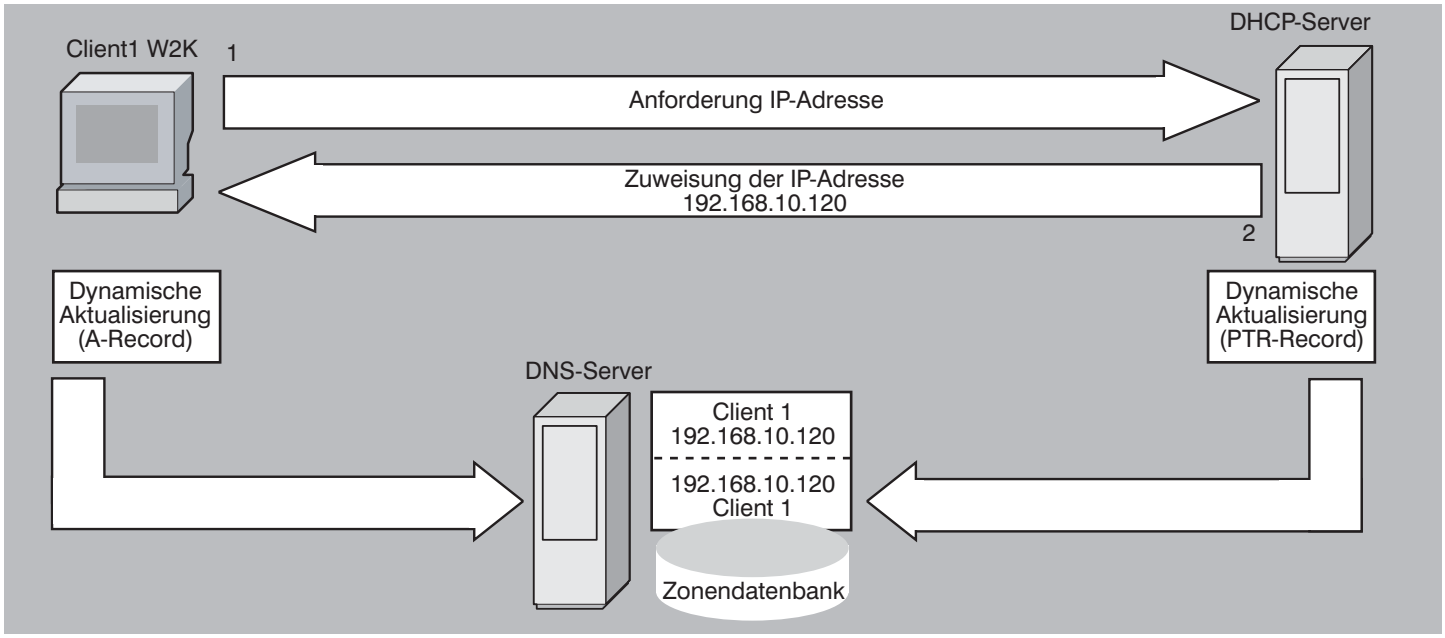


Abbildung 2: Dynamisches DNS Update durch Windows-Clients ab Windows 2000

Microsoft-Hotline angekommen, dass es einen eigenen MS-Knowledge-Base-Artikel hierzu gibt.

Bestimmte Windows-Clients (ab Windows 2000 aufwärts) können dabei Änderungen ihrer IP-Adressen selbst „einbuchen", für andere Geräte muss der DHCP-Server dies tun.

Gleich die nächste Baustelle: Zusammenwirken von DDNS und DHCP, sowie die Frage, ob DDNS-Server in einem Windows-Netz immer von Microsoft sein müssen. Das sicher nicht.

Allerdings hat eine Speicherung der DNS-Daten („Zonendatei") im Active Directory Sicherheits-Vorteile gegenüber einer Speicherung als einfache Datei, wie dies bei herkömmlichen DNS-Servern der Fall ist. Aus diesem Grund empfiehlt auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) als Maßnahme des BSI-Grundschutzes eine Verwaltung der Zonendatei innerhalb des Active Directory, wenn ein solches vorhanden ist. Damit nicht genug, Maßnahme „M 4.141 Sichere Konfiguration des DDNS unter Windows 2000" des BSI-Grundschutzhandbuchs nennt eine Reihe von Anforderungen für das Erreichen des Niveaus des BSI-Grundschutzes:

- Erfolgt eine Speicherung der Zoneninformationen als einfache Datei, so ist diese mit den Mitteln des Filesystems gezielt auf Zugriff durch Administratorkonto und den DDNS-Prozess zu beschränken.
- Es sind Vorkehrungen zu treffen, die sicherstellen, dass Zonentransfers (DNS-Server-Abgleich, Basis der Redundanz von DNS-Servern) nur zwischen „bekannten" Rechnern stattfinden. Hierzu ist eine Liste solcher Server zu pflegen und über bestimmte Sicherheitsoptionen unter Windows dafür zu sorgen, dass sich keine „Fremdlinge" dazwischenmogeln können.

Da war übrigens „en passant" die nächste wichtige Fragestellung des IT-Betriebs: Verfügbarkeit von Diensten, hier durch Redundanz von DNS-Servern sicherzustellen.

Was sind aber nun die „bestimmten Sicherheitsoptionen" unter Windows, wo stellt man sie ein bzw. kontrolliert sie? Grundeinstellungen wird man in Setup-Karten finden, Detaileinstellungen aber erfolgen über Registry-Keys. Wer sich mit dem Thema Registry bereits aktiv beschäftigt hat, wird bestätigen, dass man hier „wissen sollte, was man tut". Dies gilt in zweierlei Hinsicht: Erstens muss man die maßgeblichen Registry-Keys kennen. Wer ahnt etwa, dass sich hinter dem Schlüssel „QueryIpMatching" die sicherheitsrelevante Festsetzung verbirgt, ob ein Client auch DNS-Informationen von nicht-autorisierten Servern des Netzes akzeptiert? Zweitens ist es notwendig, die möglichen Werte zu kennen und ihre Auswirkungen. So kann ein DDNS-update etwa daran scheitern, dass eine Seite DDNS in der „secure"-Variante fährt, während die andere die unsichere Version aktiviert hat.

Man sieht am in der Idee nicht grundlegend anspruchsvollen Beispiel DDNS, dass es eine Reihe von Details gibt, die es zu beachten gilt, wenn man aktuelle TCP/IP-Mechanismen nicht nur nach Black-Box-Prinzip einsetzen, sondern wirklich beherrschen will. Das Beherrschen der eingesetzten Technik macht aber genau den Unterschied zwischen damit „Spielen" („plug and play") und professionellem Betrieb aus. Ein IT-Betreiber im Zeitalter von Service Level Agreements o.ä. Ausprägungen klarer Ansprüche an die IT-Dienstleistung auf hohem, garantiertem Niveau kann es sich nicht leisten, spielerisch mit solchen akut gewordenen TCP/IP-Techniken um zu gehen - er muss „sich auskennen" und mit diesem Wissen bewusst umgehen, in Planung, Betrieb und Trouble Shooting.

Neue Anforderungen an IP-Netzwerke, die man verschieden bedienen kann.

Hier ist etwa das Thema „Echtzeitfähigkeit" zu nennen. Dieses kommt in LAN-Umgebungen z.B. mit dem VoIP-Angebot

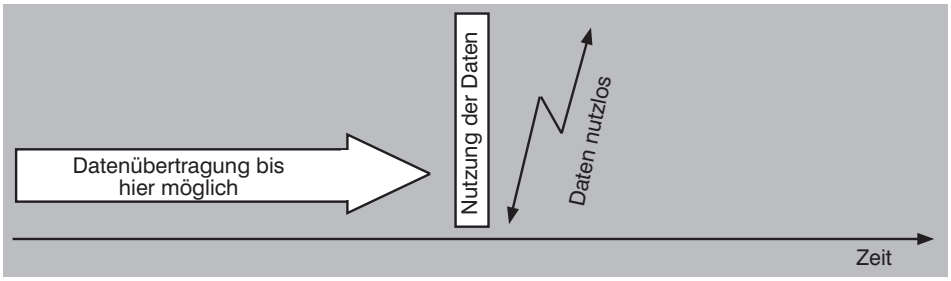


Abbildung 3: Echtzeitfähigkeit – auf das Timing kommt es an

auf die Liste. Es können aber auch bestimmte Anwendungen anderer Natur als Sprachübertragung sein, die einen besonderen Anspruch an das Eintreffen von Informationen in einem bestimmten Zeitfenster erheben.

Zum Teil extreme Anforderungen kommen hier aus dem Produktionsumfeld. Mit dem Einzug von Ethernet-Technologie (Stichwort „Industrial Ethernet“) stellt sich automatisch die Frage, in wie weit TCP/IP auch den Anforderungen der Industriekommunikation genügen kann.

Ganz so extrem muss es nicht immer zugehen, aber genau hier liegt der erste Aufgabe: die konkreten Anforderungen erfassen. So gibt es Untersuchungen mit dem Ergebnis, dass der „Durchschnitts-Telefonierer“ eine Sprachumlaufzeit von mehr als 300 ms nicht mehr als Gesprächstauglich empfinden, d.h. als schlechte bis indiskutable Qualität.

Lösungen im Bereich erhöhter Ansprüche an rechtzeitiges Eintreffen von Informationen können Quality of Service-Methoden oder eine Optimierung des Zusammenspiels der Routing-Komponenten über Zeitsynchronisierung sein. In extremen Fällen können sogar Modifikation/ Austausch der Mechanismen auf Layer 3 und 4, also IP und TCP bzw. UDP das Mittel der Wahl sein. Was wählt man im eigenen Fall?!

Den Fortschritt verstehen und ausnutzen

Weiter gilt es „auf dem Laufenden zu bleiben“, um neu etablierte „state of the art“-Ansätze nicht zu verschlafen, sie aber (s.o.) auch wirklich zu beherrschen. Hier ist zum Beispiel der Einsatz von VRRP zu nennen mit den zugehörigen Erfahrungen aus der Praxis und dem für das Trouble Shooting notwendigen Verständnis.

Auch Mobile IP ist erwähnenswert, ein Ansatz, bei dem es ermöglicht wird, den „Aufenthaltsort“, d.h. das IP-(Sub-)Netz zu verlassen, ohne dass die bisherige IP-Adresse und alle darauf aufbauenden „Sitzungen“ ungültig werden. Mit dem „alten“ Ansatz, Netzwerk-Zugehörigkeit und physikalischen Aufenthaltsort, d.h. den Netzanschluss eng miteinander zu verkoppeln, geht hier nichts. Es müssen neue Mechanismen her, ohne dass die alten wegfallen. Denn niemand wird ernsthaft erwägen, wegen des für manche interessanten Aspekts Mobilität (gerade VIP-user werden begeistert nach solchen Lösungen rufen!) auf allen Rechnern die IP-Software auszutauschen, weil die alten Kommunikationsmechanismen durch neue ersetzt werden müssen, die Mobilität zulassen.

MPLS, Quality of Service – wie sieht die Praxis aus?

Quality of Service (QoS)-Fähigkeit war einer der Vorzüge, mit dem seinerzeit ATM auch im LAN stark argumentiert wurde. Mittlerweile gibt es eine Auswahl an Lösungsmöglichkeiten, innerhalb und außerhalb von IP:

- **QoS auf Layer 2**
  Hier ist als nicht-proprietärer Ansatz nach wie vor ATM führend.

- **QoS auf Basis von Warteschlangen in Netzwerk-Komponenten**

  Die diversen Lösungen werden oft mit Hersteller-spezifischer Komponenten im Detail ergänzt. Ideal sind dabei solche, bei denen die Identifikation der mit Priorität zu behandelnden Datenflüsse auf Basis von IP-Parametern erfolgen kann. Auf diese Weise bleibt die Steuerungsinformation einheitlich, und man muss nicht planerisch und betriebstechnisch eine komplizierte Kombination verschiedener Konzepte ausbalancieren.

  Dabei bestehen durchaus grundlegende Unterschiede: etwa ob die Priorisierung

rein auf IP-Adressen und TCP/UDP-Ports o.ä. beruht und der Rest per Administration in der Komponente vorgegeben wird, oder aber der Sender eines Datenstroms die Behandlung mit Priorität erst „anfordern“ muss (via Differentiated Service Bits im IP-Header). Hier muss man als IT-Betreiber Bescheid wissen, um gezielt entscheiden, planen und parametrieren zu können.

- **QoS auf Basis dynamischer Ressourcen-Reservierung entlang des Weges**

  Die reine Warteschlangen-Behandlung in der einzelnen Komponente erfolgt auf Grundlage einer festen Parametrierung der einzelnen Komponenten: Definition der Warteschlangen und Zuordnung der Datenströme sowie Auswahl der Art von Priorisierung (bestimmte Datenströme stets vollständig zuerst, oder nur bis zu einer bestimmten Datenmenge und danach „fairer Wettbewerb“ um den Rest der Ressourcen, o.ä.). Mit einer solchen „manuellen“ Bindung von Kapazitäten für einzelne Datenströme kann aber nur mit hohem administrativem Aufwand auf Veränderungen in den Datenströmen - Flussrichtung und Ressourcen-Anforderungen - reagiert werden.

  Hier hat ein Verfahren wie das Ressource Reservation Protocol RSVP den Charme, eine dynamische Vereinbarung zu Beginn der Datenübertragung zu erlauben. Auch diese Rose hat aber natürlich Dornen in Form typischer Fragen wie:

  Was passiert, wenn die Reservierung mangels Kapazitäten in den fraglichen Routern fehlschlägt? Reagiert das Verfahren dann „beleidigt“ und es ist Schluss mit der Priorisierung, so dass man Ressourcen „im Überfluss“ planen muss? Kann hier (dynamischer Mechanismus!) womöglich eine neue Security-Problematik entstehen? Was ist, wenn auf dem Kommunikationsweg nicht alle Router gleichermaßen RSVP unterstützen? Wie sieht es aus über Strecken mit langen Laufzeiten, kann die Reservierung womöglich Timer-bedingt hieran scheitern?

- **Realisierung über Class of Service-Unterscheidung mittels MPLS**

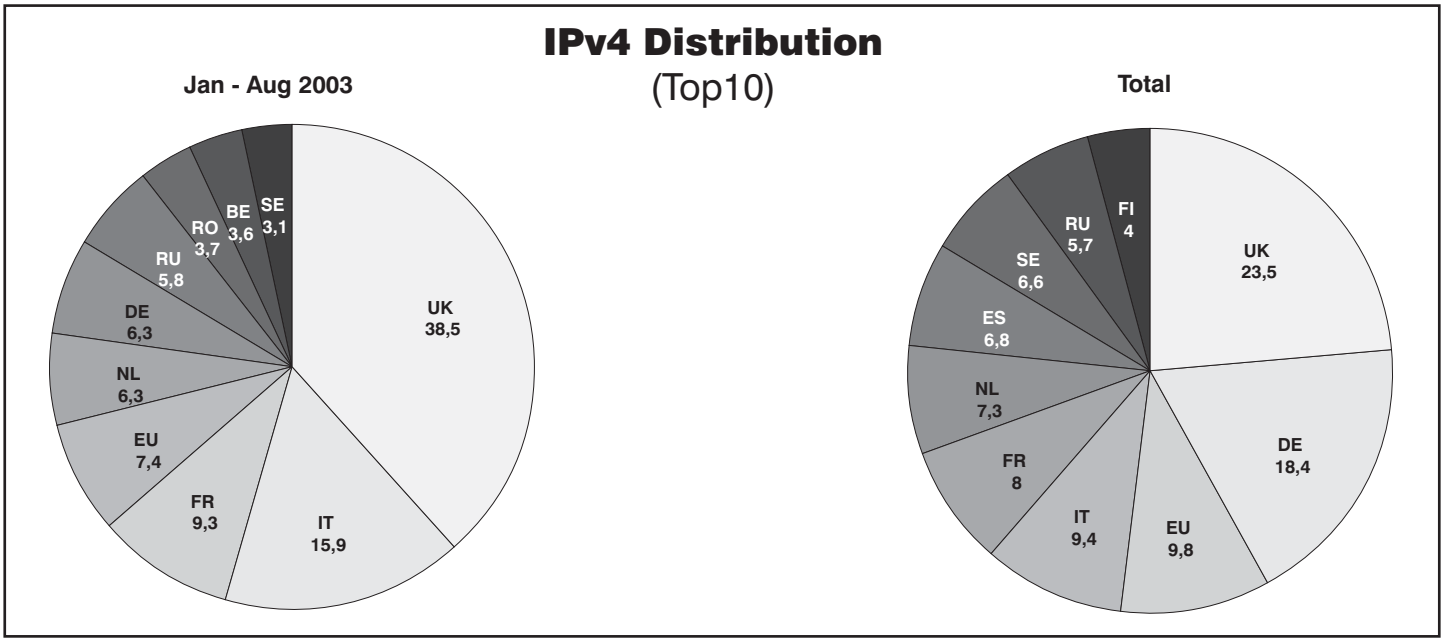
  Von allen Ansätzen, mit denen man mit Aufkommen der neuen, leistungsstarken Layer 2-Switches die Routing-Komponenten Performance-technisch retten wollte, ist der des „Label-Switching“ in Form von MPLS übrig geblieben – heute jedoch als add-on zum normalen Routing, das man bei Bedarf bewusst dazuschalten kann. Über bei Eintritt in eine „MPLS-Wolke“ den Paketen beigegebene Label-Information können die MPLS-fähigen Komponenten innerhalb der Wolke schnelle Entscheidungen für den Transport treffen, insbesondere auch eine Priorisierung zur Realisierung verschiedener Classes of Service. Klingt gut, hat ja fast die Qualität von Layer 2-Switching hinsichtlich auf die Dauer der Transportentscheidung - zumindest innerhalb der MPLS-Struktur.

Welcher Ansatz ist nun der in der Praxis richtige? Erfahrene Netzwerker werden es ahnen: „die“ Lösung gibt es nicht, man muss für den konkreten Fall und die eigene Umgebung die verschiedenen Möglichkeiten gegeneinander ausloten, womöglich sogar geschickt kombinieren - und dazu muss man sich auskennen. Es gilt abzuwägen, welcher Mechanismus am besten zu den Anforderungen passt, und wo Aufwand/Kosten am günstigsten sind. Meist muss man Planungsaufwand und -häufigkeit gegen Betriebs- und Trouble Shooting-Aufwand abwägen.

Die „immer grüne“ Frage: Kommt IPv6 nun oder kommt es nicht?

So heiß, wie dieses Thema mal Mitte/Ende der 90er Jahre gehandelt wurde, ist es sicherlich nicht. Die erste Welle der Produktankündigungen mit IPv6-Unterstützung rührte im Nachhinein betrachtet wohl daher, dass niemand der Letzte sein wollte. Die Knappheit registrierter IPv4-Adressen wurde vor allem durch die Kombination von NAT und Proxy-Lösungen entschärft - aber eben nur entschärft.

Auch wenn es als sportliche Herausforderung sicherlich interessant ist, wie lange man mit Tricks und Erweiterungen von Übersetzer-Ansätzen zwischen Netzen, die sich direkt „nicht sehen dürfen“ noch auskommt, kann dies nicht als idealer Zustand für den Betreiber von Net-zen angesehen werden. Es handelt sich eben nicht um eine „never change a winning team“-Situation, wenn IPv4 trotz der Verfügbarkeit von IPv6 aktiv gehalten wird. Vielmehr wird permanent an IPv4 herumgeschraubt: noch immer sind nicht alle



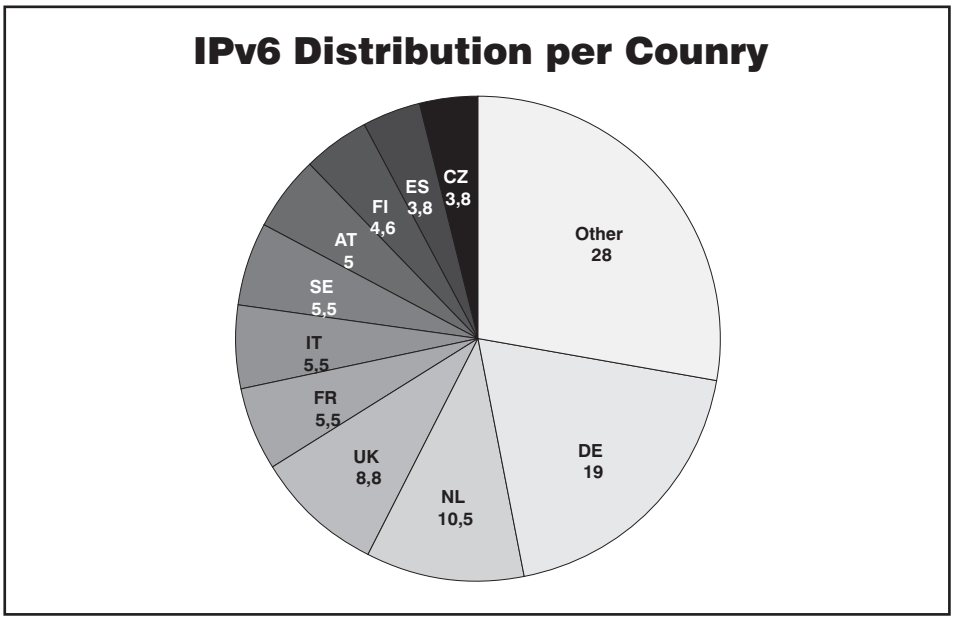


Abbildung 4 und 5: Anteile an IPv4- bzw. IPv6-Installationen (Quelle: Ripe NCC)

Kommunikationsformen über NAT möglich, und Themen wie Security oder QoS sind unter IPv4 mühseliger unterzubringen als unter IPv6.
Teilweise wurden sie bei IPv6 im Gegensatz zu IPv4 bei der Entwicklung bereits berücksichtigt; bei der Entwicklung von IPv6 wurde Wert darauf gelegt, notwendige Ergänzungen „elegant" über optionale Header aufnehmen zu können. Dies zeigt sich etwa am Beispiel Mobile IP, das unter IPv4 im Vergleich zu IPv6 stellenweise an eine Notlösung erinnert.

Ein Festhalten an IPv4 „mit Gewalt" birgt verschiedene Gefahren:

- **„Spaghettiprogrammierung"**

  Selbst wenn die Erweiterungen an bestehenden Lösungen „sauber" entworfen sind, muss dies noch lange nicht für die Realisierungen in den IP-Stacks gelten. Es droht die in der Software-Entwicklung immer wieder (gerade unter Zeitdruck) auftretende „Spaghetti-Programmierung" mit den bekannten negativen Auswirkungen.

- **Verleitung zu betriebstechnisch ungünstigen Lösungen**

  Gerade das Thema NA(P)T und Kopplung von Netzen, die nicht direkt miteinander kommunizieren dürfen bzw. können, ist auch eine Achillesferse. Wer schon einmal erlebt hat, was es bedeutet, zwei Unternehmensnetze zu koppeln, die zuvor beide mit demselben Adressvorrat gestartet sind, kann ein Lied davon singen.

Eine Migration tut natürlich weh, stellt aber genauer betrachtet vielleicht das „Ende mit Schrecken" dar, das dem betriebstechnischen „Schrecken ohne Ende" im Sinne der IT-Stabilität und Verfügbarkeit vorzuziehen gewesen wäre.

Mit IPv6 hat sich das Thema auch langfristig erledigt, da der Vorrat an registrierten Adressen keinen Grund mehr gibt, überhaupt überschneidende Adressmengen zu erleben.

Dies soll kein Plädoyer sein, nun „endlich und sofort" auf IPv6 über zu wechseln. Dies wäre praxisferner und unvernünftiger Aktionismus.

Man sollte jedoch die Entwicklung im Auge behalten und insbesondere eine bewusste Entscheidung treffen können, ob

und wann ein Übergang auf IPv6 im eigenen Netz günstig ist. Die meisten werden immer noch keine wirkliche „Ahnung haben“, was denn an IPv6 anders ist als an IPv4 oder wo die Produktentwicklung aktuell steht und was sich konkret ändert bei einem Übergang.

Dabei hat sich eine Menge getan, und dies nicht zuletzt in Deutschland: der Anteil an IPv6-Installationen hat im europäischen Vergleich in Deutschland überproportional zugenommen, wie die Graphiken (Quelle: RIPE NCC) zeigen (Abbildung 4 und 5).

Vieles hat sich zu IPv6 herauskristallisiert, was längere Zeit offen war und sicherlich zu den entscheidenden Fragen für Planung und Betrieb zu zählen ist. Die „best practice“-Strategie zur Adressraumstrukturierung ist klar: ein definierter Anteil für die hierarchische Netzwerk-Identifizierung, der Rest zur „freien Gestaltung“, dabei z.T. Ableitung der Adress-Eindeutigkeit aus den zugrundeliegenden MAC-Adressen. Die Produktverfügbarkeit ist mittlerweile auch gegeben, etwa unter Windows (Mehrzahl der betroffenen IP-Stacks!) oder unter Linux, „dem“ Thema der letzten Monate. Wenn man sich mit entsprechenden Installationen beschäftigt, wird man feststellen, dass sich im wesentlichen die unteren Schichten beim Übergang auf IPv6 verändern, während die Dienste darüber ohne besondere Konfigurationsänderung wahlweise auf IPv4 oder IPv6 (bzw. parallel) laufen.

Womöglich liegt hier im Zeitalter der Verlagerung auch von IT-Aufgaben ins Ausland für das von Innovativität und Know-How abhängige Deutschland eine Chance. Dies gilt aber bestimmt nicht, wenn man aus Bequemlichkeit oder Angst die anderen machen lässt, um dann als Nachzügler auf den Zug aufzuspringen.

Schließlich noch: Multicast-Routing

Dieses Beispiel steht ganz bewusst am Schluss. Es zeigt sowohl, wie uralte Ideen plötzlich im Fahrwasser entsprechender Anforderungen aus dem Anwendungsbereich vom scheinbar „toten Ast“ zum schnell an Bedeutung wachsenden Trieb werden können (dasselbe kann mit IPv6 geschehen, sobald sich eine entsprechende Initialanwendung durchsetzt, z.B. im Bereich Mobilität). Es zeigt auch, dass ein Arbeiten „von der Stange“ oder „plug and play“ leicht zu ungünstigen Entscheidungen führen kann, die den insgesamt zu bedienenden Anforderungen Performance, Stabilität und Flexibilität nicht standhalten.

Wer ist sich dabei sicher, dass das Thema für ihn jetzt und in Zukunft keines ist? Anwendungen für Multicast-Routing sind Anwendungsformen, deren Nutzen stark von einer quasi-Gleichzeitigkeit des Empfangs einer Sendung bei mehreren Empfängern abhängen: Video- oder Audio-Streams, Video-Konferenzen, Telefonkonferenzen, Informationsdienste wie Börsenticker o.ä.

Das Neue ist hier die Streuung der Empfänger über das ganze physikalische Netz. Die Multicast-Group der an einem solchen Datenstrom Interessierten kann mit einem über das Gesamtnetz verstreuten logischen Subnetz verglichen werden.

Sofort ergeben sich Fragestellungen wie Redundanz ohne Schleifen, Beschränkung des Multicast-Traffics auf die notwendigen Netzbereiche (Vorsicht: Switching hilft hier nicht oder nur mit Zusatzmechanismen!) und die Wahl des optimalen Routing-Verfahrens völlig neu. Flutungs-Verfahren mit nachträglichem Beschneiden des netzumspannenden Routing-Baums („Tree-Pruning“) gegenüber Ansätzen über Routing-Bäume mit Rendevouz-Punkten, in die man sich bei Bedarf einbucht, erfordern auch für „alte Hasen“ ein mühsames Hineindenken. Ebenso die Bestimmung des Routing-Trees: „Umkehrung“ eines bekannten Routing-Verfahrens (RIP bei DVMRP oder OSPF bei MOSPF), oder vielleicht lieber ein „Protocol Indipendent Multicast“-Routing (PIM), um nicht auf ein einheitliches unicast-Routing-Protokoll im ganzen Netz angewiesen zu sein? Hier sind wieder gezielte Entscheidungen zu treffen, was nur in Kenntnis der Ansätze und ihrer Vor- und Nachteile sinnvoll möglich ist.

Fazit:

Auch wer ein stabil laufendes, neu eingerichtetes IP-Netzwerk betreibt, kann und sollte sich auf diesen Lorbeeren nicht ausruhen. Allerdings ist es mühselig, sich umfassend auf dem Laufenden zu halten, und es droht die Gefahr, sich zu verzetteln oder die Zähne an schwer lesbaren IETF-Veröffentlichungen (Drafts oder RFCs) auszubeißen.

Hier bietet die ComConsult Akademie Interessierten eine Alternative: auf Basis von Recherche und Projektwissen erfahrener Mitarbeiter der ComConsult Beratung und-Planung GmbH entsteht ein Seminar, das zu den genannten und weiteren aktuellen Themen Einblick und erste Einordnungen gibt. Es soll helfen, sich selbst eine Meinung zu bilden - zu Detailfragen oder dazu, in welche Themen man für die eigene Umgebung gezielt als nächstes einsteigen sollte. Dieses Seminar trägt den selben Titel wie der vorliegende Artikel - allerdings im Sinne des Artikelinhalts ohne das Fragezeichen: „Neues bei TCP/IP“.

Studie des Monats Ethernet in Industrie-Umgebungen

Ethernet in der Industrie zieht in Konsequenz ein völliges Redesign der Produktions-Netzwerke nach sich, das bis in die vorhandenen Backbone-Strukturen der Unternehmen reicht. Betroffene Unternehmen brauchen dazu zwangsläufig ein tragfähiges Rahmenkonzept, wollen sie nicht von isolierten Bastel-Projekten überrollt werden.

Hier setzt der neue Top-Report von Com-Consult-Research an. Er analysiert die bestehenden Aufgaben, bewertet die notwendigen Eigenschaften von Komponenten und erarbeitet einen neuen Design-Rahmen für Ethernet in der Industrie. HINDA ist das neue Schlagwort des Jahres 2004: Hierarchical Industrial Network Design and Architecture.

Harte und weiche Echtzeit

Derart unterschiedliche Rahmenbedingungen und Einsatzformen von Informationsflüssen legen unterschiedliche Anforderungen an Echtzeitfähigkeit nahe, denen bedarfsgerecht nur auf Basis eines abgestuften Echtzeit-Begriffs entsprochen werden kann.

Eine Abstufung muss auch vorgenommen werden, um zu vermeiden, dass man in bestimmten Bereichen mit den sprichwörtlichen Kanonen auf Spatzen schießt. Da sich zumindest hohe Echtzeitanforderungen nicht ohne weiteres mit Ethernet und TCP/IP realisieren lassen, können Lösungen, welche die geforderten Eigenschaften besitzen, nicht billig sein. Solche High-end-Technik in Bereichen einzusetzen, in denen geringere Anforderungen zu erfüllen sind, ist nicht wirtschaftlich.

Entsprechend werden bei den Ansätzen zur Definition von Echtzeit auch bewusst verschiedene Stufen unterschieden.

Eine verbreitete grundlegende Abstufung stammt von der IAONA. Sie unterscheidet zunächst zwischen harten und weichen Echtzeitanforderungen, kurz auch harter bzw. weicher Echtzeit.

Basis dieser Definitionen ist eine Betrachtung, wie viel eine Information je nach Zeitpunkt des Eintreffens noch wert ist. Dies kann formal in einem so genannten time/utility-Diagramm dargestellt werden, in dem der Nutzen (engl. utility) in Abhängigkeit von der Zeit eingetragen wird. Voller Nutzen erhält den Nutzwert 1, eine zum Betrachtungszeitpunkt nicht mehr sinnvoll verwertbare Information wird mit 0 bewertet.

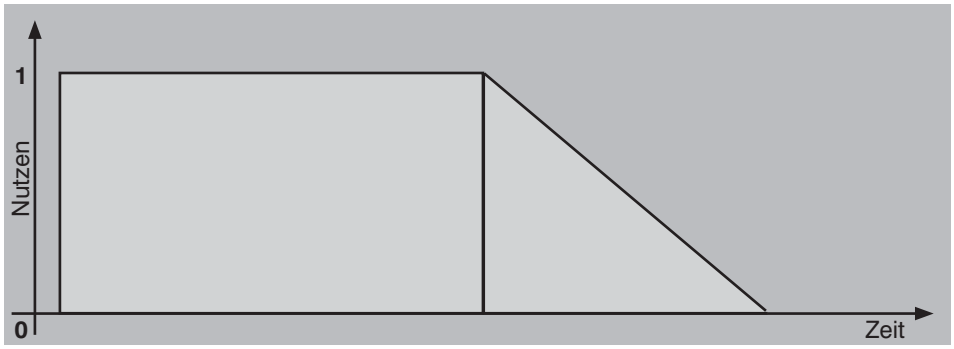


Abbildung: Zeit/Nutzen-(time/utility-) Diagramm für weiche Echtzeit

Weiche Echtzeit ist nun dadurch charakterisierbar, dass die gesendete Information bis zu einem eindeutigen spätesten Zeitpunkt beim Empfänger eintreffen muss, so dass dieser sie noch rechtzeitig verwerten kann. Nach diesem Zeitpunkt nimmt der potenzielle Nutzen aus Sicht der Anwendung, die die Information verwerten soll, stetig ab, bis irgendwann die Information völlig wertlos geworden, da sie viel zu spät eingetroffen ist.

Das Weiche an dieser Echtzeitforderung besteht darin, dass die Information nicht sofort völlig wertlos wird, sobald eine bestimmte Zeitschranke nicht eingehalten wird. Eine darüber hinaus eintretende Verspätung kann durch die Applikation in Grenzen noch kompensiert werden. Das Eintreffen im vorgesehenen Zeitrahmen ist hier zwar in hohem Maße wünschenswert, aber nicht zwingend erforderlich, um eine Störung zu vermeiden.

Bei harten Echtzeitanforderungen hingegen ist die Information sofort wertlos, wenn sie nicht in einem bestimmten Zeitraum eintrifft; die Kurve des time/utility-Diagramms wechselt entsprechend abrupt zwischen 1 und 0 als Nutzenwert. Hier gibt es verschiedene Fälle:

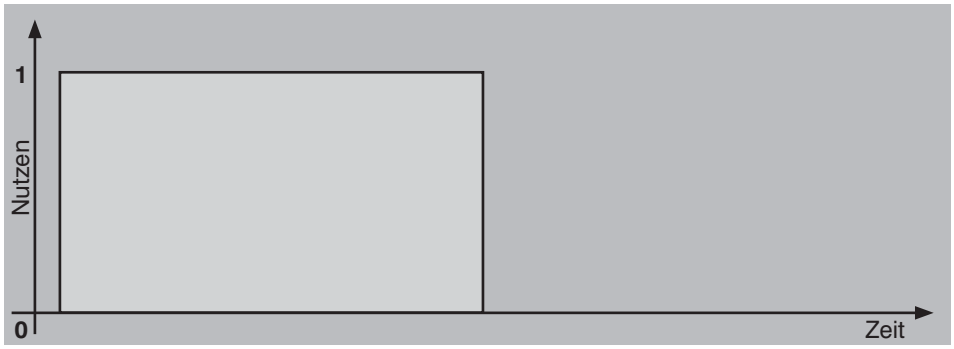


Abbildung: Zeit/Nutzen-Diagramm für harte Echtzeit mit oberer Schranke

- harte Echtzeit mit oberer Schranke
  Hier ist der Nutzen gewahrt, solange die Information bis zu einem bestimmten spätesten Zeitpunkt beim Empfänger eintrifft. Diese Anforderung lässt sich mit schnellstmöglicher Übertragung erfüllen.
- harte Echtzeit mit oberer und unterer Schranke
  Die zu erfüllende Anforderung ist hier schärfer: ein bestimmter Jitter um den-

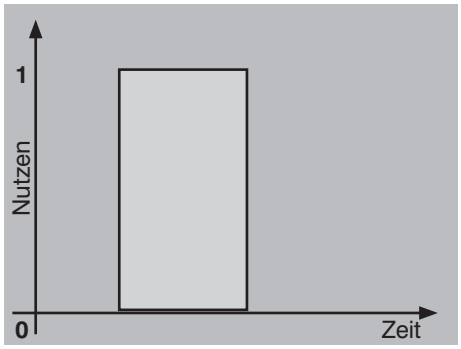


Abbildung: Zeit/Nutzen-Diagramm für harte Echtzeit mit oberer und unterer Schranke

optimalen Empfangszeitpunkt darf nicht überschritten werden. Die Information darf weder zu früh noch zu spät eintreffen.

Natürlich ist eine Vorgabe im Sinne der Definitionen von weich und hart nur dann eine Echtzeit-Anforderung, wenn die Realisierung eine echte Herausforderung an die Technik darstellt, die über das in Büronetzen Normale hinausgeht. Theoretisch ist auch eine harte Echtzeit mit oberer und unterer Schranke denkbar, bei der Zeitraum zwischen diesen Schranken Minuten oder gar eine Stunde beträgt. Eine solche Festlegung wäre jedoch für die Lösungs- oder Anforderungskategorisierung zu Industrienetzen ohne jeden Wert.

Die Praxis zeigt, dass im Bereich der harten Echtzeit mit oberer und unterer Schranke sinnvoll mehrere Stufen zu unterscheiden sind, um für verschiedenste Anwendungen, wie z.B. Abfüllanlagen oder große Druckereien, eine bedarfsgerechte Realisierung zu ermöglichen. Eine entsprechende genauere Betrachtung mit unterschiedlichen Sollwertbereichen folgt in Kapitel 2.5.3. Die höhere der beiden entsprechenden Echtzeit-Klassen stellt z.T. so hohe Anforderungen an die Genauigkeit der Übertragung, dass die heute typischen Realisierungsformen nur mit Zusatzmechanismen wie Synchronisierung der Teilnehmer die Anforderungen erfolgreich realisieren können.

Für die zuvor unterschiedenen Kommunikationsebenen ergibt sich in etwa die folgende typische Verteilung der Echtzeitanforderungen:

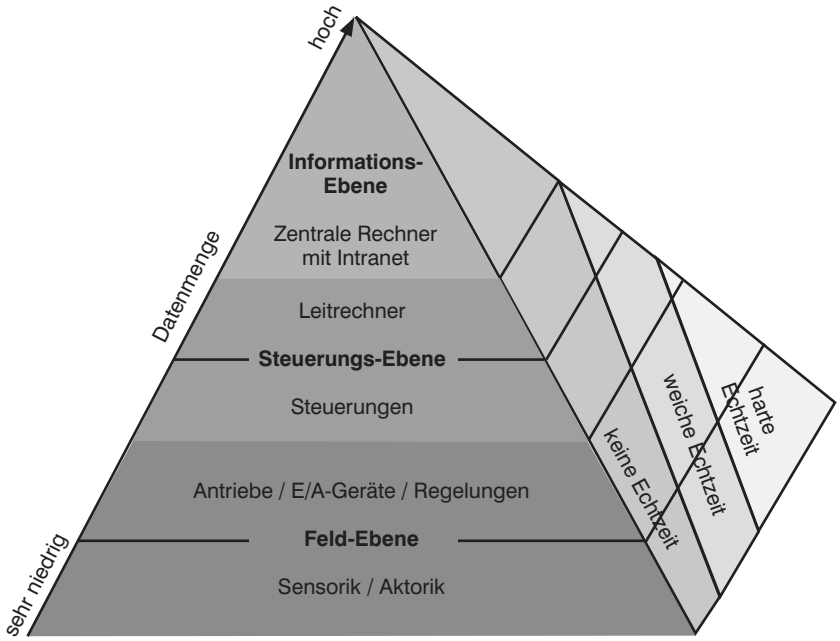


Abbildung: Potenzielle Echtzeit-Anforderungen der Kommunikationsebenen

Schwerpunktthema

Session Initiation Protokoll bringt neue Bewegung in den Voice over IP Markt

Fortsetzung von Seite 1

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

1. Was ist SIP und wozu braucht man es?

Was macht SIP zu einer so wichtigen Entwicklung? Der HTTP Standard hat dadurch, dass er die Ablage auf zentralen Servern und den Zugang zu Webseiten für Endgeräte standardisiert hat, eine Revolution des Internet vom Text-Medium hin zum Präsentaitons-Medium bewirkt. SIP hat das Potenzial, in ähnlicher Weise die Realzeit-Kommunikation für alle Arten von IP-Geräten zu revolutionieren, egal ob Mobil-Telefon mit GSM oder WLAN, IM-fähige Geräte, PDA, Softphone oder Hardphone. SIP ermöglicht ein neues Maß an Interoperabilität und durch Nutzung globaler Konzepte (IP-Adressen, E-Mail-Adressen, DNS) ein neues Maß an Skalierbarkeit. Wesentliche Verbesserungen des SIP-Modells im Vergleich zum klassischen TK-Modell sind:

- Verlagerungen der Kontrolle der genutzten Dienste ins Endgerät (dadurch Vermeidung zentraler Switches und Senkung der Entwicklungskosten durch Nutzung von Web-Interfaces)
- Flexibilität (eine Session kann Sprache, Video, Messaging oder auch ein Spiel sein)
- Erweiterbarkeit (durch die definierte Nutzung anderer Protokolle können neue Protokolle leicht eingebunden werden)
- Integration mit wichtigen und weit verbreiteten Internet Standards (Nutzung und Unterstützung von URI, MIME, DNS) bei gleichzeitiger Rückwärts-Kompatibilität erweiterter Spezifikationen (SIMPLE) zu vorhandenen Spezifikationen (SIP)

Kernaussage 1: Das Potenzial zur revolutionären Veränderung der Realzeit-Kommunikation liegt in der Einfachheit und Flexibiltät von SIP sowie in der Nutzung von weltweit etablierten Webstrukturen.

Die strategische Sichtweise

SIP ist das erste Protokoll, das ernsthaft das Potenzial hat, auf der Basis von Webkonzepten Interoperabilität und Konvergenz für öffentliche und Enterprise Netze, verkabelte und drahtlose Netze herzustellen.

Die taktische Sichtweise

SIP unterstützt die Einführung neuer Nachrichten- und Konferenzdienste, indem es Informationen über Anwesenheit und Aufenthaltsort eines Benutzers in diese Dienste einbindet und die Interoperabilität zwischen den verschiedenen Mediastreams Sprache, Daten und Video / Multimedia erhöht.

Die technische Sichtweise

SIP ist ein Layer-7 Protokoll, und zwar ein Signalisierungs-Protokoll zur Kontrolle von Sessions in einem IP Netzwerk. Eine Session kann dabei alles von einem einfachen bidirektionalen Telefonanruf bis hin zur kollaborativen Multimedia-Session sein. Anders gesagt: SIP ist eine von mehreren Möglichkeiten, Sprach-, Video- und Nachrichtenkommunikation zwischen zwei oder mehr Endgeräten aufzubauen. Anfänglich beschränkt auf die Nutzung für IP Telefonie, weitet sich der SIP-Einsatz auf verschiedene neue Bereiche wie Erweiterung von Telefonie-Anwendungen, Konferenzen, Video, Instant Messaging, Anwesenheitsanzeige und Kollaboration aus.

Die SIP Sichtweise entspricht der allgemeinen Internet Sichtweise: Intelligente Endgeräte kommunizieren direkt miteinander und nutzen dabei eine simple Transport-Infrastruktur. Dies steht in krassem Gegensatz zum traditionellen Telefonie-Netzwerk, in dem die Kommunikation zwischen dummen Terminals („Handapparate“) durch ein intelligentes Kernnetz (d.h. Netzverbund von Telefonswitches) geleistet wird, das aktiv an jeder Verbindung beteiligt ist. Dieser Unterschied ermöglicht es, dass als Netzwerk nur noch „Otto-Normal-Intelligenz“ benötigt und im Prinzip jedes SIP-Gerät, das an das Netzwerk angeschaltet wird, für alle anderen SIP-Geräte Dienste anbieten kann. Das wiederum bildet eine Grundlage für verstärkten Wettbewerb, sinkende Preise und schnelle Innovationszyklen. Im traditionellen intelligenten Telefonnetz dagegen kann nur die Telefongesellschaft neue Dienste anbieten, was eine Hochrüstung der Telefonswitches erfordert, was wiederum ein langsamer und teurer Prozess ist.

1.1 Wie entwickelt sich der Markt und was treibt ihn?

Nach der Dell Oro Group wurden 2,6 Millionen IP-Telefonie Anschlüssen in Q4/2003 verkauft; damit betrug das Wachstum in diesem Quartal weltweit 19%, davon jedoch 89% außerhalb von Nordamerika. Das bedeutet: nach einer Vorreiterphase der USA holen die restlichen Industrieländer jetzt auf. Über das gesamte Jahr 2003 gerechnet haben IP PBX Systeme ihren Marktanteil im Enterprise TK-Markt verdoppelt. Die Marktführer im Q4/2003 nach

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

Anschlusszahlen waren
- Alcatel (24% Wachstum)
- Avaya (64% Wachstum)
- Nortel (32% Wachstum)
- Cisco (27% Wachstum)
- Mitel (25% Wachstum)
- Siemens (41% Wachstum)

Kernaussage 2: Die allgemeinen Marktstudien belegen, dass der Voice over IP Markt aktuell einer der wenigen Märkte mit starkem Wachstum ist.

Von Infonetics Research liegt eine Studie aus Q4/2003 vor, die Komponenten wie ATM Switch Voice Gateways, Class 5 PSTN Switches, konvergente PSTN Switches, RAC VoIP Gateways, Media Server, Session Border Controller, TDM und IP Softswitches und TK-Applikationsserver weltweit, für Nordamerika, EMEA und Asien/Pazifik erfasst. Die Studie kommt zu folgenden Ergebnissen:

- Media Gateways:13 % Umsatz-Wachstum auf 745 Mio. USD in 2003
- Softswitches: 31 % Umsatz-Wachstum auf 380 Mio. USD in 2003
- TK-Anwendungs Server: 9 % Rückgang auf 33,7 Mio. USD in 2003
- IP PBXen: 33 % Umsatz-Wachstum auf 256 Mio. USD in 2003
- IP PBXen: Prognose von 830 Mio. USD in 2007, d.h. ein CAGR von 34 %
- Anzahl der IP Anschlüsse bei Hybridanlagen: 52 % Wachstum in 2003
- Anzahl der IP Anschlüsse bei reinen IP PBXen: 29 % Wachstum in 2003
- Anzahl IP Anschlüsse von Hybridanlagen: 68 % aller verkauften IP Anschlüsse in 2003
- „Next Generation Products“: 21 % Wachstum in 2003
- „Next Generation Products“: 31 % Wachstum in Q4/2003
- „Next Generation Products“: Prognose von 305 % Wachstum bis 2007 auf 5 Mrd. USD, d.h. ein CAGR von 42 %

Die TIA ist mit ihrem „Telecommunications Market Review and Forecast“ über verschiedene Marktsegmente, der sich Netzwerk-Dienste, Enterprise und Consumer, Mobilfunk und Drahtlose Kommunikation untersucht, zu ähnlich interessanten Wachstums- und Umsatz-Ergebnissen gekommen:

- Umsatz-Wachstum von 7,8 % in 2004 auf 13,9 Mrd. USD
- Umsatz von 18,7 Mrd. USD in 2007, d.h. 9,7 % CAGR
- Umsatz-Wachstum für Audiokonferenz, Videokonferenz, Webkonferenz, Follow Me, UM und IM von 696 Mio. USD in 2003 auf 1,5 Mrd. USD in 2003
- Umsatz-Prognose für Audiokonferenz, Videokonferenz, Webkonferenz, Follow Me, UM und IM von 11,4 Mrd. USD für 2007, d.h. 66,5 % CAGR
- 58 % des gesamten Netzverkehrs in 2003 war IP, mit einer Wachstums-Prognose von Faktor 6, d.h. mit 1,633 Peta-Byte / Monat in 2007 ein CAGR von 58,3 %

Marktführer wie Microsoft und AOL haben SIP-Unterstützung implementiert oder angekündigt. Das 3GPP adaptiert SIP.

Ein offener Punkt ist noch das Thema Regulierung im TK-Markt: Hier gibt es eine Ankündigung von FCC Chairman Michael Powell, das VoIP-basierte TK-Dienste nicht mit der Steuer belegt werden, die für klassische TDM Carrier festgelegt ist. Ein Memo vom Februar 2004 besagt, dass die FCC VoIP Provider möglicherweise verpflichten will, Notrufdienste (E911) einzurichten und eine minimale Regulierung zu praktizieren. Gleichzeitig hat die FCC eine Erklärung abgegeben, dass Pulver.Com‘s Free World Dialup VoIP Dienst weder ein TK-Dienst noch Telekommunikation war und daher nicht unter die Regulierungsbestimmungen fällt (!).

1.2 Erreichbare Geschäfts-Vorteile

Ein Beispiel: T-Systems will ihr komplettes Netz bis Mitte 2005 auf Voice over IP umstellen und ist eine Partnerschaft mit VocalTek eingegangen. Alle neue Dienste und Geschäftsmöglichkeiten sieht das Unternehmen im Zusammenhang mit IP: VPN, WLAN Roaming für Hotspots, SMS-F und andere. BT in Großbritannien und Sonera in Finnland sind mit SIP-basierten Diensten im Rollout.

Kernaussage 3: Das große Versprechen von SIP ist, TK-Anwendungen von teurer proprietärer Hardware zu lösen – sowohl für zentrale TK-Switches als auch für Endgeräte.

Die Attraktivität für SIP für neue Providerdienste liegt darin, dass SIP im Gegensatz zu SS7, H.323 oder MGCP Codecs, Medium und Sessionparameter nicht innerhalb von SIP festlegt sondern existierende Verfahren und Protokolle nutzt. Somit ist SIP vom unterliegenden Transportnetzwerk unabhängig, und ein Provider kann Sprach-, Video- und Maildienste über ein komplett neues Medium wie Wireless LAN oder UMTS sofort implementieren, während er bei SS7 oder MGCP erst auf eine neue Protokollversion warten müsste, die dieses Medium unterstützt bzw. einbindet. Da die SIP Syntax HTTP-ähnlich ist, können Anwendungs-Entwickler etablierte Programmierschnittstellen wie JAVA und XML nutzen, um neue Anwendungen zu realisieren, während Carrier früher auf eine Einzelfunktion wie Call-Waiting oder Caller-ID mit SS7 jahrelang warten mussten.

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

Vonage, ein Provider für den Markt kleiner Unternehmen und privater Verbraucher, betreibt mehr als 20.000 Anschlüsse für Telefonie und Voice Mail mit SIP. Delta Three, sowohl Hersteller von Telefonprodukten als auch Service Provider, bietet auf Basis SIP eine PC-Telefon Lösung an, mit der PC-Anwender weltweit jedes beliebige Telefon anrufen können. Denwa Communications bietet für PC-PC und Telefon-PC als Dienste Anrufanzeige, Voice Mail, Konferenzschaltung, UM, Account Management, selbstinitiierte Freischaltungen und webbasierte Personalisierung – alle Dienste mit SIP.

Vorteile, die sich beim Einsatz von SIP für Unternehmen ergeben können, sind:

- Nutzung eines Standards mit der entsprechenden Produktbreite und zukünftig Ineroperabilität
- Vereinfachtes Kommunikations-Netzwerk für den Betrieb von Sprache, Daten und Video
- Hohe Flexibilität bei der Auswahl von Wählverfahren, Endgeräten und Betriebskonfigurationen
- Unterstützung von remote Arbeitsplätzen mit der Funktionalität von TK-Nebenstellen
- Skalierbarkeit
- Reduzierung der Systemkosten
- Hohes Potenzial für die schnelle Einführung neuer Dienste
- Konsistenz über weltweit verteilte Organisationen hinweg, aufgrund einheitlicher Wähl- und Zugangsverfahren für Filialen, SOHO, Teleworker und mobile Mitarbeiter

1.3 Aktuelle Markttrends in der SIP-Entwicklung

Konsumer Markt

SIP hat das Glück, zusammen mit dem Übergang der IP-Telefonie vom Nischenmarkt zum Massenmarkt in den Produktzyklus Eingang zu finden. Während einige der schon länger im IP-Telefonie-Markt engagierten Hersteller noch hartleibig auf H.323 fokussiert sind (z.B. Innovaphone, Telnet, Tiptel) unterstützet eine Reihe von Consumer Telefonen, die seit 2002 auf den Markt gekommen sind, schon kein H.323 mehr sondern stattdessen SIP, in manchen Fällen ergänzt durch MGCP (z.B. 8x8, BCM, D-Link, Inter-Tel, IpDialog, Mitel, Polycom, Zultys, Zyxel). Softphones etablierter Hersteller wie Ubiquity, Xten, Zultys sind reine SIP-Lösungen. Schon sind SIP-Softphones als Freeware erhältlich (z.B. Ubiquity Java-basiert, Zultys auf Linux). Auch IP-Adapter (ATA) für analoge Telefone sind für den Consumer-Markt erhältlich.

Zwar setzt die Nutzung von IP-Telefonie mit guter Qualität höhere Bandbreite als ISDN voraus, aber die DSL-Technologie (in USA auch Kabel-Modem-Technologie) hat sich inzwischen so weit etabliert, dass im Regelfall von der Verfügbarkeit ausreichender Bandbreite ausgegangen werden kann: Immer mehr Carrier (wie Dyad Digiphone, Rubicon IPNet, Talk Amerika, Vonage, bieten für den Consumer Markt IP-Telefoniedienste auf SIP-Basis an:

- IP-Telefonie für SIP-Telefone über Web
- IP-Telefonie für analoge Telefone über ATA
- IP-Telefonie per Softphone-Download (on demand, gegen monatliche Gebühr von 10 USD)
- Centrex-Dienste auf SIP-Basis
- Kostenfreie Telefonie zwischen SIP-Telefonen

Die Minutenpreise für Gespräche mit PSTN-Telefonteilnehmern sind deutlich unter denen der internationalen Telecom-Tarife, z.B. landesintern für 4 Cent/Minute, europa-intern für 5 bis 8 Cent/Minute, für 27 bis 33 Cent/Minute in so entfernte Länder wie Djibuti, Fidji Inseln, Kamerun, Mauritius, oder Oman und Sudan.

Multimedia-Anwendungen

Sowohl als Erweiterung klassischer H.323 Videokonferenz-Lösungen auf SIP als auch im Zusammenhang mit Kollaborations-Anwendungen sind erste Lösungen für multimediale Kommunikation über SIP auf dem Markt. Beispiele sind hier der Multimedia-Server MCS 5100 von Nortel (Multimedia Communication Server) oder der MXM Server von VCON (Media Xchange Manager), die beide sowohl H.323 als auch SIP und die Funktion des H.323/SIP Signalisierungs-Gateways zur Verbindung von Teilnehmern aus beiden Welten unterstützen. Die Nortel Lösung nutzt einen Sun Fire v100Server, die VCON-Lösung läuft auf Windows 2000 (ab SP3) / Windows 2003. Das Architektur-Schema des VCON-Servers ist als Beispiel in Abbildung 1.1 dargestellt. Leistungsmerkmale der VCON-Videokonferenz sind z.B.

- Rufweiterschaltung
- Rufumleitung (bei Nicht-Antwort, besetzt, generell)
- Rufaufnahme (bei Warten)
- Ad hod Konferenz
- ACD, Huntgruppen
- Wahl über Gateways (zum PSTN oder Voicemail, vereinfachte Wählroutinen)

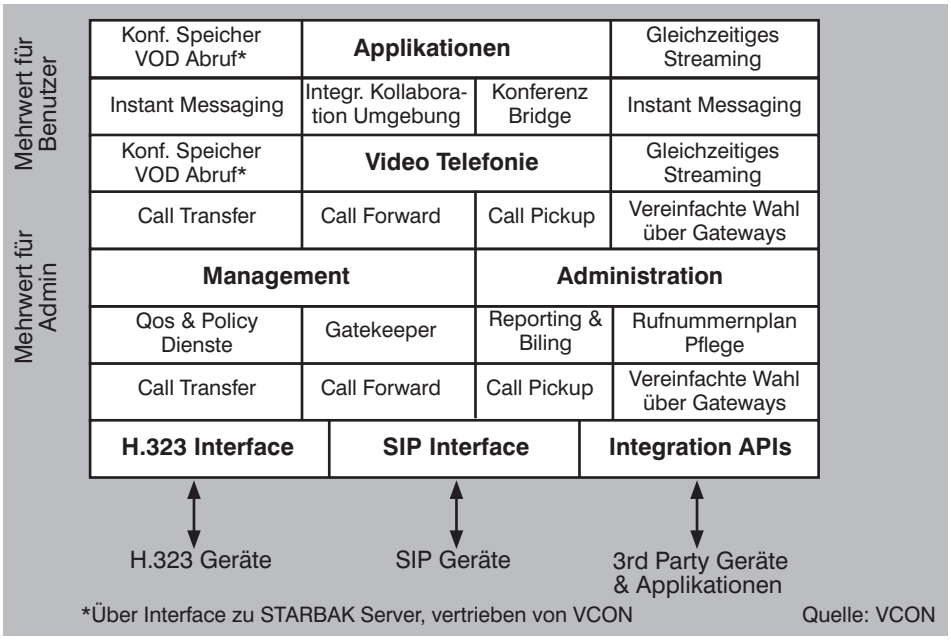


Abbildung 1.1: Architektur eines SIP-fähigen Videokonferenz-Servers

2. Die Geschichte von SIP

2.1 Geburt und Taufe

Die Anfänge von SIP liegen etwa in 1996, als ein akademisches Projekt sich um die Kontrolle der Verteilung von Multimedia Multicast entwickeln sollte.Die ersten SIP-Anwendungen implementierten eine einfache Methode, Teilnehmer zu einer Multicast Session „einzuladen“, z.B. einem Space Shuttle Start über den M-Bone. Die Nachrichtenstruktur basierte auf SMTP in der einfachen, textuellen, erweiterbaren

Form, die E-Mail so erfolgreich gemacht hatte. Als das Interesse an Internet Telefonie wuchs, wurden die Ergebnisse dieses Projekts die Basis eines neuen Protokolls, das als SIP im März 1999 von der IETF im RFC 2543 standardisiert wurde. Die ersten SIP Produkte wurden von Venture Capital Firmen mit gut abgesichertem Hintergrund entwickelt. MCI Worldcom, Cisco und ETSI TIPHON schlossen sich an, das Interesse an SIP wuchs explosionsartig. Etwa 2000 entschied sich 3GPP (Third Generation Mobile) für SIP als Basisprotokoll für seine Kommunikationsinfrastruktur. Daraus entwickelte sich erhebliche Triebkraft, die benötigten SIP-Erweiterungen für Mobilfunk zu standardisieren. Aktuelle Arbeitsschwerpunkte der SIP-Standardisierer sind NAT Traversal, Konferenz und Sicherheit.

2.2 „Born to be wild" – die Enttäuschungen

Nachdem die erste Standardisierung sich auf SIP für Telefonie (SIP-T) konzentriert hatte, wurde bald klar, dass RFC 2543 erweitert werden musste, um neue Anforderungen erfüllen zu können. Die große Anzahl von Erweiterungen, die vorgeschlagen wurden, überflutete die IETF SIP-Arbeitsgruppe und führte zu einer langen Verzögerung der Standardisierung. Das Ergebnis war, das die Standardisierung den Anforderungen immer mehr hinterherhinkte und neue Funktionen in den Produkten proprietär implementiert wurden. Dies führte zu Inkompatibilitäten bei allem, was über die Basis-Standards hinausging. Der anfängliche SIP-Enthusiasmus fiel mit der Internet-Blase zusammen, und es schien, als ob SIP einen schnellen Weg anbieten könnte, das bestehende teure PSTN-Netzwerk zu ersetzen. Optimistische Darstellungen der Funktionsmöglichkeiten von SIP führten zu unrealistischen Anforderungen an den Leistungsumfang der Produkte. Es entstanden viele SIP-Implementierungen verschiedener Standard-Versionen und Vorversionen, in den verschiedensten Programmiersprachen und mit erheblichen Unterschieden in der Vollständigkeit der unterstützten Funktionen. Das Resultat waren ernsthafte Interoperabilitäts-Probleme und Bedenken, ob SIP sich überhaupt für den kommerziellen Einsatz eignet. Diese „schlechte Presse" hätte SIP ins Abseits befördern können. Aber aufgrund sowohl seiner fundamentalen Stärken als auch mächtiger Sponsoren wie Cisco, Microsoft und Nokia hat es überlebt. Die Interoperabilität wurde durch so genannte SIPit Events des SIP Forums stetig verbessert, wenn auch deren Ergebnisse nicht-öffentlich bleiben.

2.3 Erstes Reifestadium

Schließlich wurde in 2002 der RFC 2543 durch einen Satz von Standards ersetzt, die auf dem RFC 3261 basieren. Seit Ende 2003 erscheinen die ersten Produkte auf dem Markt, die RFC 3261 unterstützen, wenn auch noch nicht in allen Teilen. Wesentliche Verbesserungen von RFC 3261 waren

- Beseitigung von Unklarheiten
- Erweiterungen
- Skalierbarkeit
- Sicherheitsfunktionen

Aktuell ist im SIP Produktumfeld die notwendige Weiterentwicklung hinsichtlich Stabilität, Sicherheit und Managebarkeit erkennbar, aber SIP muss immer noch als eine junge Technologie bezeichnet werden.

3. SIP Komponenten und Arbeitsweise

3.1 Überblick und Basis-Standards

SIP entspricht der IETF Philosophie: „Specify only what you need to specify". Im Fall von SIP heißt das: SIP wurde nur dafür gebaut, Sessions einzurichten, zu erweitern und abzubauen, es kennt die Details einer Session nicht sondern überlässt dies einem anderen Protokoll. Auch in anderen funktionalen Bereichen (z.B. Transport Protokoll, Codec, Namensdienst, remote Einwahl, Verzeichnisdienst, Sicherheit etc.) gehört es zum SIP Prinzip, auf bereits vorhandene Protokolle zurückzugreifen, soweit dies möglich ist, anstatt wie H.323 eine vertikale Integration dieser Funktionen in den SIP Protokollstack zu versuchen.

Das Protokoll ist ein Request-Response Protokoll und hat große Ähnlichkeit mit zwei sehr erfolgreichen Internet Protokollen: HTTP und SMTP. Mit SIP wird Telefonie „einfach eine weitere Web-Anwendung", die leicht in andere Internet-Dienste integrierbar ist. Genau wie H.323 nutzt SIP den Stack IP / UDP oder IP / TCP und setzt auf diesen Basis-Protokollen mit RTP, RTCP (wie H.323) oder zusätzlich RTSP auf. Da SIP selbst als „zuverlässiges" Protokoll (mit eigenem Quittungsmechanismus) arbeitet, ist es davon unabhängig, ob unterliegend UDP oder TCP genutzt wird. Zur Übermittlung der Session-Parameter nutzt SIP ein weiteres Protokoll , das SDP (Session Description Protocol, RFC 2327). Zur Authentifizierung kann RADIUS eingesetzt werden, als Verzeichnisdienst LDAP, für zusätzliche QoS-Funktionen RSVP.

Somit ist SIP die Signalisierungs-Komponente in einem insgesamt sehr modularen Ansatz für IP Telefonie und Multimedia-Kommunikation.

3.2 SIP-Architektur und Funktionen

SIP kontrolliert Sessions für einfache Telefonanrufe, Konferenzrufe (nur Sprache oder Multimedia) und Multimedia Verteilung. Teilnehmer einer Session können über Unicast , vermaschten Unicast oder Multicast kommunizieren. Mittels SDP verständigen sich alle Teilnehmer auf die genutzten Mediastreams und Mediatypen. Mobilität wird mittels Proxy- und Redirect-Diensten unterstützt. Im Gegensatz zu H.323 ist keine explizite Konferenzkontrolle bei SIP spezifiziert. Hier müsste analog zu SDP ein separates Protokoll eingebunden werden, wofür es jedoch aktuell noch keinen IETF Standard gibt. Für die Namensauflösung wird DNS genutzt, SIP Domänen sind wie DNS Domänen aufgebaut. Ein einfaches SIP-Szenario zeigt Abbildung 3.1. SIP-Adressen sind wie E-Mail Adressen aufgebaut, einige Beispiele sind in Abbildung 3.2 dargestellt.

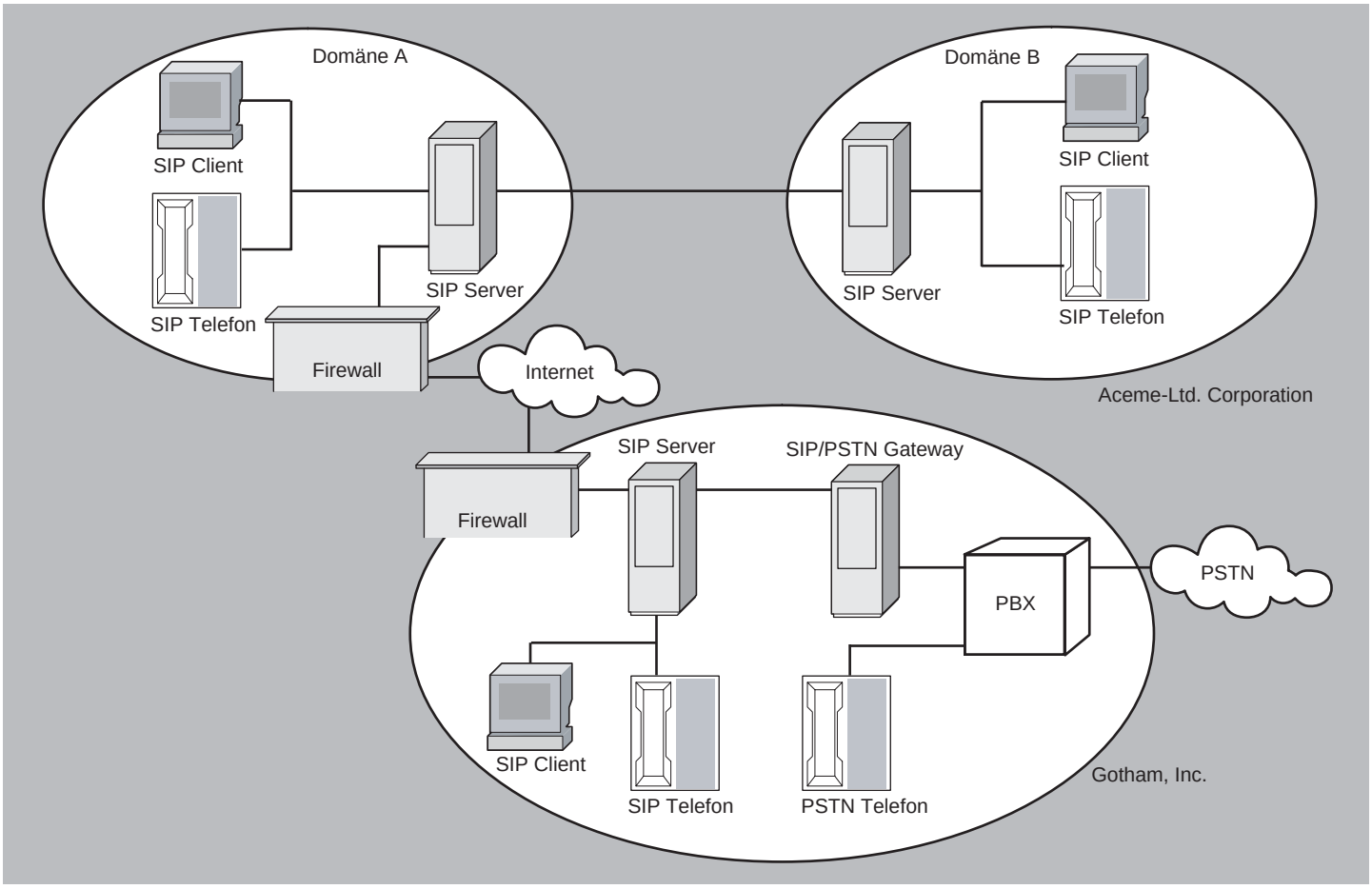


Abbildung 3.1: SIP Einsatzszenario

SIP URL Format	Erklärung
sip:donald.duck@aceme-ltd.com	Einfacher SIP URL
sip:donald@aceme-ltd.com;transport = tcp	Einfacher SIP URL mit TCP als Transport Protokoll (Default ist UDP)
sip:donald@172.16.02.54	SIP URL mit IP Adresse
sip:+49-241-955500@ubn.de;user=phone	SIP URL mit globaler Telefonnummer
sip:sales@aceme-ltd.com;maddr=225.0.2.1;ttl=64	SIP URL mit Multicast Adresse, die den vorher spezifizierten Host Namen überschreibt. TTL steht auf 64 (0 .. 255). TTL muss bei Multicast gesetzt werden, ebenso muss UDP genutzt werden.

Abbildung 3.2: Beispiel-Formate für SIP Adressen

Die SIP-Architektur ist eine Client-Server Architektur mit zwei Komponenten: dem SIP User Agent und den SIP Network Servern. Der User Agent läuft auf dem Endgerät und handhabt hier den Sessionaufbau für ausgehende und ankommende Anrufe, indem er sie als Anfragen oder Antworten an den nächsten SIP Server sendet. Die Network Server handhaben den Aufbau und die Steuerung dieser Sessions innerhalb des Netzwerks, indem sie die Anfragen / Antworten für ausgehende und ankommende Anrufe dem für die Gegenseite zuständigen Server beantworten. Es gibt verschiedene Server-Typen, die später näher erläutert werden. SIP Server entsprechen in etwa der Funktion des Gatekeepers in H.323.

Der User Agent besteht aus zwei Modulen, dem User Agent Client (UAC), der vom

SIP Client ausgehende Anfragen handhabt, und dem User Agent Server (UAS), der Anfragen an den SIP Client beantwortet (siehe hierzu Abbildung 3.3).
Eine Hauptaufgabe der SIP Server ist die Auflösung von Anfragen nach Namen bzw. Telefonnummern (Name Resolution) mittels Mapping auf die vom jeweiligen Benutzer aktuell genutzten IP-Adressen. Ist der Benutzer gerade unterwegs und befindet sich nicht am Standort seiner Domäne, kommt das Auffinden des Benutzers (User Location) als weitere Aufgabe für SIP hinzu, bevor die Namensauflösung abgearbeitet werden kann. Beschreiben wir einen möglichen Sessionaufbau mit Namensauflösung, bei der der gerufene Teilnehmer nicht in seiner Home Domäne eingeloggt ist. Eine Übersicht zeigt Abbildung 3.4.

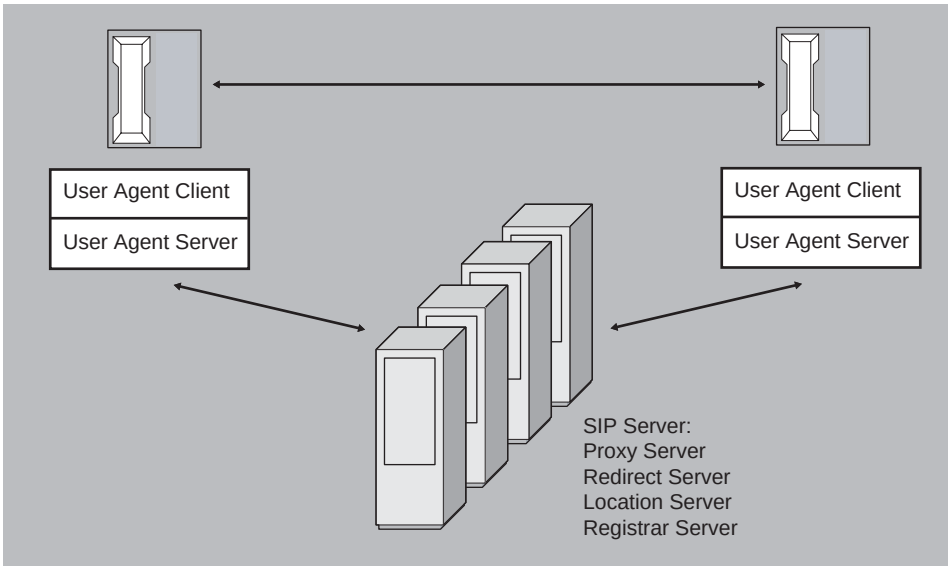


Abbildung 3.3: Komponenten des SIP User Agent und SIP Server

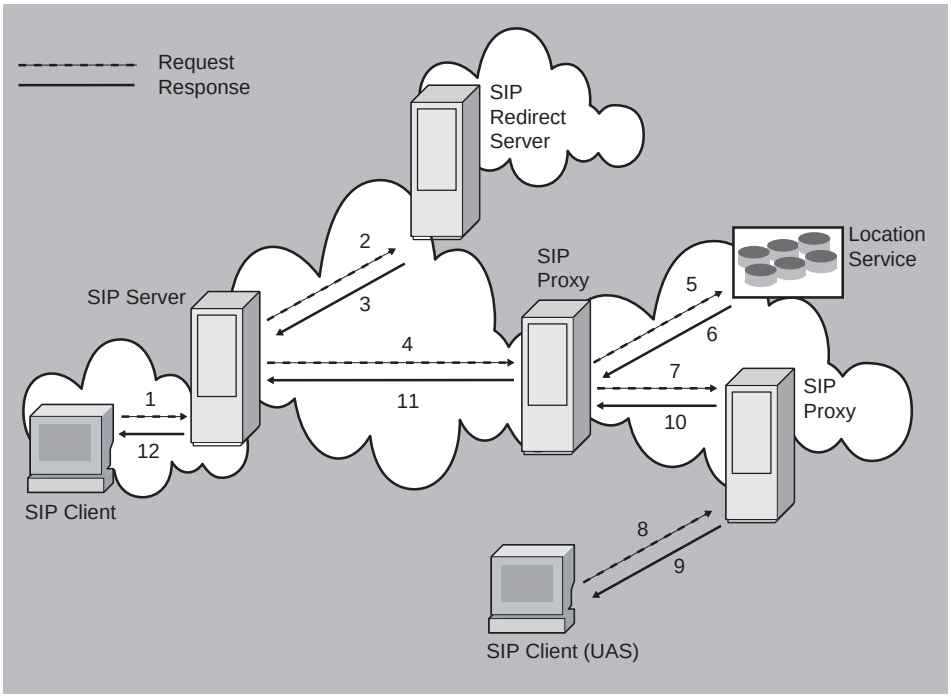


Abbildung 3.4: Namensauflösung mit SIP

1. Ein SIP User Agent generiert einen INVITE Request für sip:joe@company.com. Der Request wird an einen lokalen Proxy weitergeleitet.
2. Der Proxy löst joe@copany.com über DNS auf und erhält die IP Adresse eines SIP Servers für diese Domäne. Er spricht in seiner Funktion als Proxy den SIP Server an.
3. Der Server für company.com kennt Joe, aber der ist gerade als j.user@university.edu eingeloggt. Also leitet der Server den Proxy auf diese Adresse um.
4. Der lokale Proxy löst university.edu mit DNS auf und erhält die IP Adresse seines SIP Servers. Der Request wird mittels Proxy-Funktion an diesen weitergeleitet.
5. Der Universitäts-Server fragt eine lokale Datenbank an
6. Die Datenbank gibt zurück, dass j.user@university.edu lokal als j.smith@cs.university.edu bekannt ist.
7. Der Universitäts-Server gibt als Proxy den Request an den Computer Science Server weiter.
8. Dieser Server kennt die IP Adresse, unter der der Benutzer gerade eingeloggt ist
9. Der Benutzer „Joe“ nimmt den Anruf an und die Antwort wird über die gebildete Proxy Kette zurück zum Anrufer geleitet: 9, 10, 11, 12.

Die Funktionen, die SIP mit der beschriebenen Architektur realisiert, sind

- Name-Translation und User Location: stellt sicher, dass der Anruf das Ziel erreicht, egal wo sich der Angerufene befindet; es erfolgt Mapping aller möglichen Namensbeschreibungen (URL, E-Mail u.a.) auf den aktuellen Standort / die IP Adresse
- Auswahl der Leistungsmerkmale und Session-Parameter (Feature negotiation): ermöglicht es den Teilnehmern eines Anrufes, sich darauf zu einigen, welche Leistungsmerkmale unterstützt werden, auch wenn nicht alle Teilnehmer alle Merkmale unterstützen
- Wechsel der Session-Parameter: Auch währen eines Gesprächs sollte es einem Benutzer möglich sein, einzelne Parameter und Leistungsmerkmale zu ändern (z.B. von reinem Audio auf Audio plus Video)
- Management der Rufteilnehmer: Während eines Anrufs können z.B. einzelne Teilnehmer hinzukommen, die Teilnahme beenden, weitergeschaltet oder auf „Parken“ gesetzt werden

Mit diesen Funktionen können SIP Endgeräte und SIP Proxyserver die typischen eines Telefondienstes erfüllen und handhaben:

- User Location (Auffinden des gerufenen Teilnehmers)
- User Capabilities (Aushandeln der Leistungsmerkmale)
- User Availability (Feststellung der Er-

reichbarkeit)
- Call Setup (Anrufaufbau)
- Call Handling (Anrufsteuerung)
- Call Forwarding (Fwd) mit
  - Bedienung von Notrufnummern
  - Fwd No Answer (Weiterleitung bei Nichtannahme)
  - Fwd Busy (Weiterleitung bei Besetzt)
  - Fwd unconditional
  - Weitere Adress-Translation Dienste wie parallele Mehrfach-Weiterleitung u.a.
- Callee und Calling Number Übermittlung mit verschiedenen Namensschemata
- Mobilität (Single Access)
- Anzeige und Auswahl des Terminal-Typs
- Auswahl der Terminal-Funktionen
- Authentifizierung des anrufenden und angerufenen Teilnehmers
- Überwachte und nicht-kontrollierte Weiterschaltung (Transfer)
- Einladung zu einer Multicast Konferenz

3.3 SIP Server

Die SIP Spezifikation (RFC 3261, früher RFC 2543) teilt die SIP Server Funktionalität in drei Unterfunktionen auf:

- SIP Registrar Server
- SIP Redirect Server
- SIP Proxy Server

Diese Unterteilung wurde von den SIP-Erfindern weniger als Implementierungs-Richtlinie sondern mehr für ein leichteres Verständnis getroffen. Es ist daher ohne weiteres möglich, mehrere oder alle drei Funktionen auf einem einzigen „SIP Server“ zu implementieren. Darüber hinaus ist es durchaus nicht unüblich, auf dieser Box noch weitere Funktionen zu implementieren wie Routing, PSTN-Gateway, Signalisierungs-Gateway oder ähnliches. Sogar ein SIP Endgerät bzw. der darauf laufende SIP User Agent darf zusätzlich Serverfunktionen unterstützen, zum Beispiel dürfen User Agenten Anfragen oder Registrierungen umleiten.

Der SIP Registrar Server

Der Registrar Server handhabt den Location Dienst für eine Domäne. Hierfür akzeptiert er REGISTER Requests und pflegt die so erhaltenen Informationen in einer (abstrakten) Location Datenbank ein, genannt „Location Dienst“. Der Location Dienst kann lokal oder remote implementiert sein, der Zugriff kann im letzteren Fall ein separates Protokoll wie LDAP nutzen. Läuft der Location Dienst remote, wird er manchmal als „Location Server“ bezeichnet. Der SIP Standard gibt hier nichts vor, sondern überlässt diese Entscheidung der jeweiligen Implementierung (siehe hierzu Abbildung 3.5).

SIP Clients generieren REGISTER Requests, um ein Mapping ihrer (extern) bekannten SIP Adresse auf die aktuell gültige IP Adresse einzurichten oder zu löschen. Der REGISTER Request kann auch genutzt werden, um alle verfügbaren Mappings für eine spezielle Adresse abzufragen.

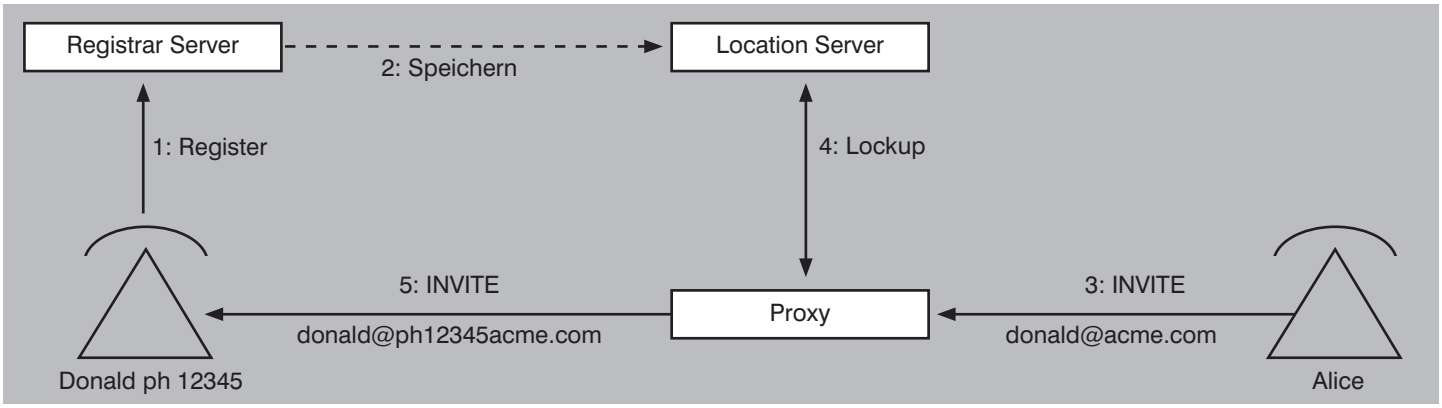


Abbildung 3.5: Registrierung und zugehörige Aktionen bei SIP

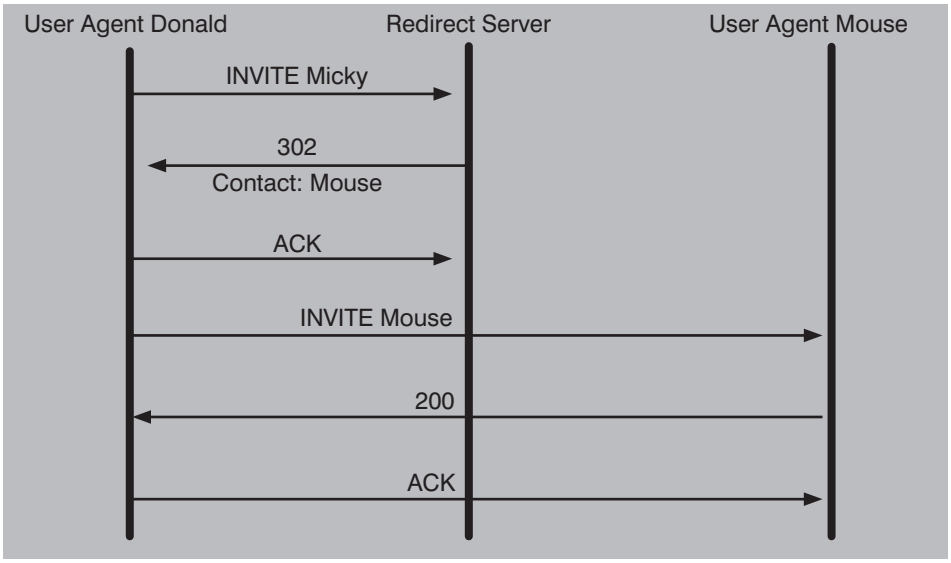


Abbildung 3.6: Umleitung eines INVITE Requests mittels Redirection bei SIP

Der SIP Redirect Server

Der Redirect Server hat den einfachsten Job: Er empfängt SIP Requests und antwortet mit 3xx Code Responses (Redirection, siehe weiter unten). Auf diese Weise dirigiert er den Client oder Client Request um, damit eine andere SIP Adresse kontaktiert wird. Diese alternative(n) SIP Adresse(n) werden in der Redirect Antwort Nachricht als so genannte Contact Header zurückgeliefert. Ein Ablaufschema ist in Abbildung 3.6 dargestellt.

Der SIP Proxy Server

Der SIP Standard beschreibt den Proxy Server als eine Komponente, die „SIP Requests zu User Agent Servern (UAS) und SIP Responses zu User Agent Clients routet“. Ein Request kann auf seinem Weg

zum UAS mehrere Proxy Server durchlaufen. Jeder Proxy Server trifft Routing Entscheidungen und ändert den Request entsprechend, bevor er ihn an die nächste SIP Komponente weiterleitet. Die Antworten durchlaufen in umgekehrter Reihenfolge dieselbe Proxy Server Abfolge wie die Requests.

Eigentlich können Proxy Server als „SIP Router" beschrieben werden (auch wenn das den Cisco Router Freaks unter den Lesern weh tut), die SIP Anfragen und SIP Antworten weiterleiten. Allerdings ist die angewendete Routing Logik ausgefeilter als ein simpler Routing Tabellen Lookup. Proxy Aktionen umfassen nämlich auch Request-Validierung, Benutzer-Authentifizierung, Fork Prozesse, Adress-Resolution, Abbruch offener Session-Aufbauten und Loop-Behandlung. Die aus dem Routing bekannten Optionen Record Route und Loose Route sind für „SIP Routen" ebenfalls definiert.

Proxy Server lassen sich je nach Einsatzbereich weiter in Typen unterteilen wie Edge Proxy (z.B. für SOHO), Enterprise Proxy (im Unternehmens-RZ) und Core Proxy (im Provider Backbone). Darüber hinaus sind Proxy Server so definiert, dass sie für Endsysteme, d.h. User Agents im wesentlichen transparent arbeiten:

- Proxy Server dürfen SIP Nachrichten nur nach speziellen Vorgaben und Limitierungen ändern: Ein Proxy darf z.B. den SIP Body einer Nachricht nicht ändern
- Proxy Server dürfen mit einigen wenigen Ausnahmen nicht eigeninitiativ INVITE Requests generieren
- Ebenso kann ein Proxy Server eine Session nicht mit einem selbst-generierten BYE Request beenden

SIP Proxy Server können auf zwei verschiedene Arbeitsmodi konfiguriert werden: den stateful Modus und den stateless Modus. Im stateless Modus bearbeitet ein SIP Server die Requests, speichert jedoch keine Informationen darüber, was die Skalierbarkeit erheblich steigert. SIP Server, die innerhalb eines Netzwerk-Backbones positioniert sind, arbeiten daher besser im stateless Modus, da sonst eine zu hohe CPU-/Speicherleistung erforderlich wäre, und der stateful Modus innerhalb eines Backbone keinen besonderen Nutzen bietet.

Im stateful Modus merkt sich ein SIP Proxy eine Anfrage (Anrufer, Zeitpunkt, Ziel, Dauer u.a.), daher ist dieser Modus im Netzzugangs-Bereich oder bei Netzübergängen zwischen Providern sinnvoll. Hier muss ein einzelner Server nicht so viele Anfragen bearbeiten, so dass seine CPU- und Speicherleistung nicht überfordert wird. Zudem ist hier der netztechnisch sinnvolle Punkt für Nutzung der Informationen zu Abrechnungszwecken.

Ein stateful Proxy bearbeitet eher komplette Transaktionen als einzelne Nachrichten: Server Transaktionen, um Requests zu empfangen und Antworten zurückzuliefern, Client Transaktionen, um Requests zu senden und Antworten zu empfangen. Die Kernfunktion eines Stateful Proxies (Proxy Core Object) ist es, Assoziierungen zwischen Client und Server Transaktionen herzustellen und so den Gesamtzustand eines Requests zu verwalten. Die Proxy Kernfunktion wählt die Zieladressen aus und initiiert entsprechend eine oder mehrere Client Transaktions-Instanzen. Außerdem sammelt sie die Antworten verschiedener Client Transaktionen und entscheidet, welche davon sie upstream als Server Transaktion sendet (siehe Abbildung 3.7).

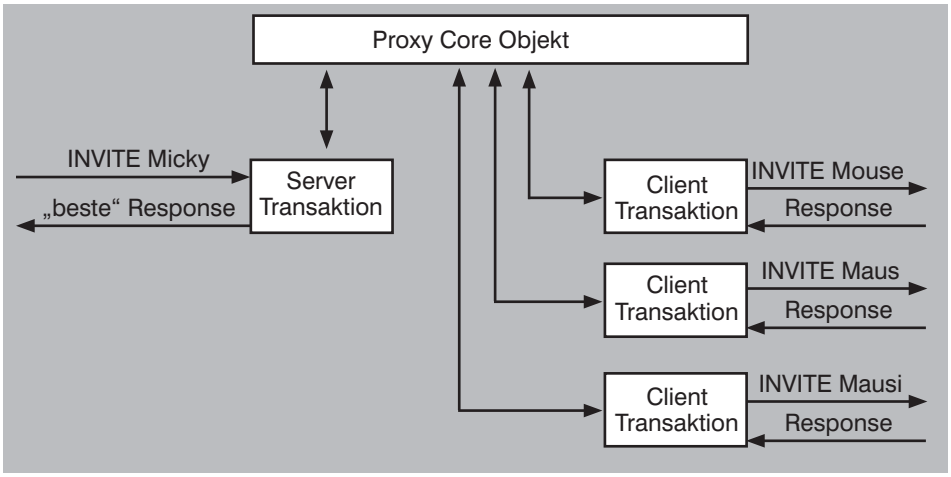


Abbildung 3.7: Stateful SIP Proxy Server Modell

Ein stateful Proxy kennt den jeweiligen Stand einer Transaktion und die Nachrichten-Historie, daher kann er eingehende Nachrichten auf einem höhern Informationsniveau verarbeiten als ein stateless Proxy. Zum Beispiel kann er eine Retransmission erkennen und wird diese nur in Ausnahmefällen weiterleiten, in denen eine Wiederholung erforderlich ist. Ein stateless Proxy muss dagegen alle Nachrichten bearbeiten, da er nicht in der Lage ist, Wiederholungen zu erkennen. Ein stateful Proxy kann CANCEL Requests lokal bearbeiten und je nach Bedarf CANCEL Requests generieren. Ebenso sind es eher die stateful Proxies, die Forking (d.h. Vervielfältigung) für SIP Nachrichten durchführen.

Allerdings wird die Mehrfunktionalität mit einigen Nachteilen bezahlt:

- Erhöhter Speicherbedarf
- Niedrigerer Durchsatz
- Komplexere Implementierung
- Komplexerer SIP Stack
- Syntax-Überprüfung
- Überprüfung des URI Schema
- Überprüfung des Max Forwards Feld (ähnlich dem TTL Feld in IP Paketen)
- Durchführung von Loop Detection
- Bearbeiten des SIP Require feldes (hier trägt ein Client spezielle Anforderungen an Proxies ein) und Unterstützung aller Eintragungen erforderlich
- Authentifizierung

Wenn ein Proxy einen eingehenden Request validiert und sich entschieden hat, ihn weiterzuleiten, muss er bestimmen, an welche Zielsysteme die Nachricht weitergeleitet wird. Er führt zu diesem Zweck eine zweifache Adressresolution durch:

- Festlegung der Zielmenge: Der Proxy ordnet der SIP Zieladresse (Request URI) eine Menge von SIP Adressen zu, die in irgendeiner Form auf die Zieladresse gemappt sind.
- DNS Auflösung: Der Proxy mappt jede SIP Zieladresse auf eine Transport-Adresse der Form {Transport_Protocol, IP Adresse, Port}

Die DNS-Auflösung ist in RFC 3263 (SIP: Locating Servers) beschrieben und nutzt im wesentlichen die DNS-Anfragen SRV, NAPTR, A und AAAA, um eine bestimmte SIP Adresse auf eine priorisierte Menge von Transport-Adressen zu mappen. Es kann also erforderlich werden, einen SIP Request an mehr als eine Zieladresse weiterzuleiten, z.B. wenn ein Benutzer gleichzeitig an mehreren Standorten registriert

ist. In diesem Fall wird entweder sequentiell oder parallel eine Vervielfachung (Forking) des Requests durchgeführt.

3.4 Signalisierung

Die Signalisierung verwendet ein einfaches Request-Response Modell: Um einen Sessionaufbau zu initiieren, sendet der Anrufer (Client, UAC) einen „INVITE“ Request mit dem URL des gerufenen Teilnehmers. Kennt der Client den Standort des Angerufenen, kann er den Request direkt an die entsprechende IP Adresse senden. Falls nicht, sendet er ihn an einen lokal konfigurierten SIP Proxy Server. Der Client kann jedoch auch so konfiguriert sein, dass er den Request immer an den Proxy Server sendet und gar keinen direkten Versuch unternimmt.

Der Server wird versuchen, den Standort bzw. die IP Adresse des gerufenen Benutzers aufzulösen und den Request dorthin zu senden. Für die Auflösung können DNS-Server oder lokale Datenbanken herangezogen werden. Falls der Server ein Redirect Server ist, wird er eine gefundene IP-Adresse dem Client übermitteln, so dass dieser den Sessionaufbau selbst weiterführen kann. Ein Sessionaufbau kann über eine ganze Kette von Proxy und Redirect Servern laufen, bevor der gesuchte Teilnehmer schließlich gefunden wird und die Namensauflösung stattfinden kann.

Ist der gerufene Teilnehmer einmal gefunden, erhält er den Request des anrufenden Clients. Im einfachsten Fall klingelt dann sein Telefon. Nimmt der Benutzer das Gespräch an, beantwortet der UAS des SIP Agent den „INVITE“ Request mit Übermittlung seiner Leistungsmerkmale. Nimmt der Benutzer das Gespräch nicht an, werden etwa konfigurierte Weiterleitungsregeln aktiv: Das Gespräch wird z.B. auf einen Mailserver, ein IVR oder andere Apparate umgeleitet.

SIP beschränkt sich auf sehr wenige Aktionen (siehe Abbildung 3.8) mit übersichtlichen Aktionscodes, an deren erster Nummer der grobe Inhalt schon erkennbar ist und die dem HTTP ähnlich sind:

- 1xx Information (z.B. 100 Trying, 180 Ringing)
- 2xx Erfolgreich (z.B. 200 OK, 202 Accepted)
- 3xx Redirection (z.B. 301 Moved Permanently, 302 Moved Temporarily, 305 Use Proxy)
- 4xx Request Fehler (z.B. 401 Unauthorized, 403 Forbidden, 404 Not Found, 482 Loop Detected)
- 5xx Server Fehler (z.B. 501 Not Implemented)
- 6xx Globaler Fehler (z.B. 603 Decline, 604 Does Not Exist, 606 Not Acceptable)

SIP Aktions Codes (Methods)	
INVITE	Benutzer oder Dienst wird „eingeladen“, an einer Session teilzunehmen
ACK	Client hat eine finale Antwort auf einen INVITE Request erhalten
OPTIONS	Anfrage an den Server hinsichtlich seiner Funktionalität (Capabilities)
BYE	Anzeige des User Agent Client an den Server, den Ruf / Stream / die Session zu beenden
CANCEL	Abbruch eines offenen Requests
REGISTER	Der Client registriert seine Adresse an einem SIP Server
SUBSCRIBE	Der anrufende TN fordert (dauerndes) Update über die Anwesenheit des angerufenen TN
NOTIFY	Übermittlung von Status Update eines Clients/Telefons an TN, die eine Subscription auf ihn selbst haben
MESSAGE	Wird genutzt, um eine Instant Message zu senden

Abbildung 3.8: SIP Aktions-Codes

Zur detaillierteren Demonstration eines Signalisierungs-Ablaufs haben wir eine Animation des SIPCenter (www.sipcenter.com) eingebunden. Zum Abspielen benötigen Sie jedoch den Flash Player von Macromedia. In diesem Beispiel will User_1 in der Domäne here.com User_2 anrufen. User_1 kennt User_2, da beide üblicherweise zu der selben Domäne gehören. User_1 sendet daher ein INVITE an sip:user2@here.com an den lokalen Proxy Server, SIP Stateful Proxy Server_1. Proxy_1 wiederum sendet ein INVITE an einen Redirect Server, um den aktuellen Standort von sip:user2@here.com herauszufinden und auf Erreichbarkeit zu prüfen. Der Redirect Server entscheidet, dass User_2 zur Zeit nicht in der Domäne here.com eingeloggt ist, sondern heute in der Domäne there.com auffindbar ist. Der Redirect Server liefert diese Information mit einer „302 Moved Temporyrily“ Antwort

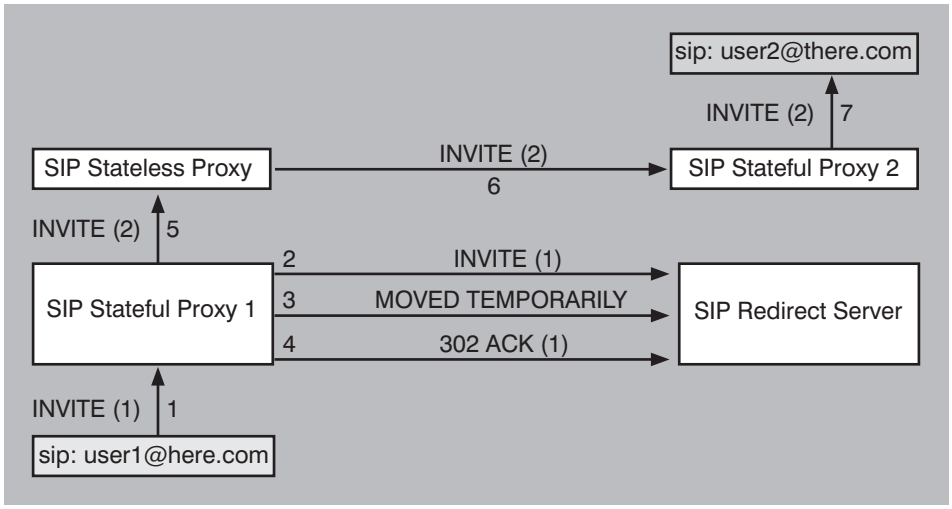


Abbildung 3.9: Beispiel für die Signalisierung eines Session Aufbaus (1)

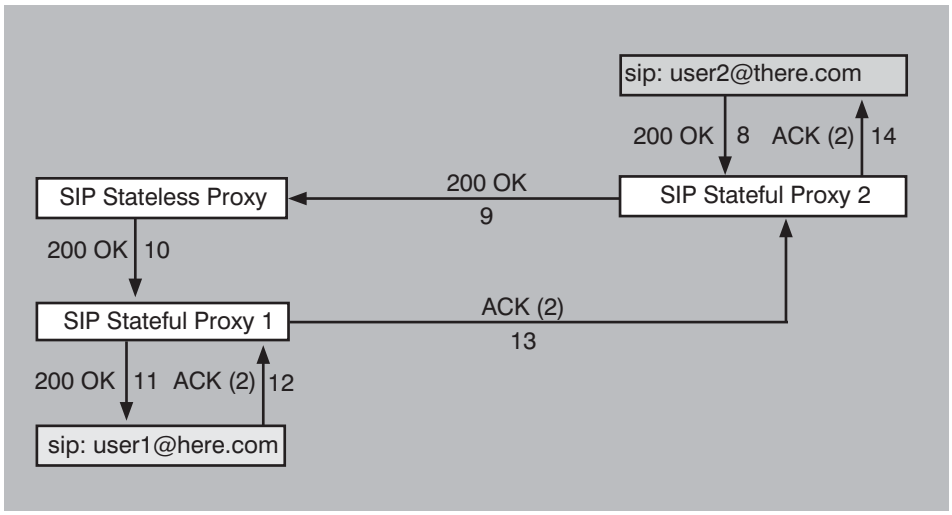


Abbildung 3.10: Beispiel für die Signalisierung eines Session Aufbaus (2)

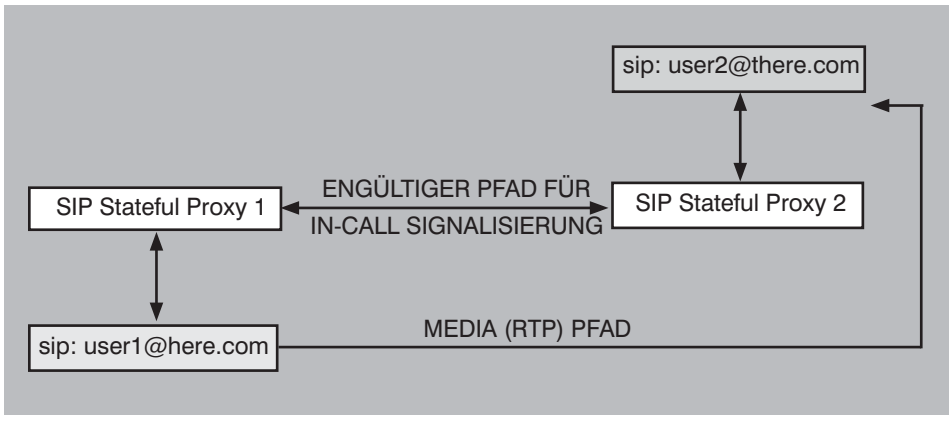


Abbildung 3.11: Beispiel für die Signalisierung eines Session Aufbaus (3)

an den Proxy_1 zurück, in der die neue Adresse von User_2 als sip:user2@there.com eingetragen ist.
Da dies eine endgültige Antwort auf den INVITE Request ist, bestätigt der Proxy_1 sie mit ACK. Er hat dann die Auswahl, die 302 Antwort direkt an User_1 zurückzuliefern, damit dieser selbst versucht, den User_2 zu erreichen, oder er kann stellvertretend für User_1 versuchen, User_2 zu erreichen. In der Animation versucht der Proxy_1, sip:user2@there.com zu erreichen, indem er einen geänderten INVITE Request sendet. Da Proxy_1 keinen anderen Proxy Server kennt, der die Domäne there.com kontrolliert, sendet er den INVITE Request an einen Stateless Proxy, der wissen sollte, wohin der Request geroutet werden muss. Der Stateless Proxy routet den Request an einen anderen Stateful Proxy Server_2, der die Domäne there.com kontrolliert. Proxy_2 findet User_2 und vervollständigt das Routing des INVITE Request. User_2 nimmt den Anruf an und antwortet mit „200 OK“. Die Antwort-Nachricht läuft über denselben Weg zu User_1 zurück wie die INVITE Anfrage. Um die Anfrage abzuschließen, muss User_1 den Empfang der Antwort mit einem ACK bestätigen. Potenziell könnte e4r das ACK direkt an User_2 senden, aber im Beispiel haben beide Stateful Proxy Server in den INVITE Requests, die sie geroutet haben, angezeigt, dass sie für die gesamte Gesprächsdauer im Signalisierungspfad verbleiben wollen. Daraus resultierend wird das ACK wieder über beide Proxies geroutet, ebenso alle weiteren SIP Nachrichten dieses Gesprächs bis zum Session-Abbau. Der Datenanteil verläuft jedoch direkt zwischen den Endgeräten (!).

Die Abbildungen 3.9 bis 3.11 zeigen den Gesamtablauf

Zur Abrundung sind in Abbildung 3.12 und Abbildung 3.13 die Formate und Inhalte einer typischen INVITE Request-Response Sequenz gezeigt.

3.5 SIP Interoperabilität mit anderen Protokollen

SIP ist eine von mehreren Protokoll-Alternativen und muss mit bereits implementierten anderen Alternativen koexistieren. Es gibt daher einen Markt für Konvertierungs-Produkte in dem einige Hersteller Signalisierungs-Gateways entwickeln. Da der größte Anteil der VoIP Lösungen in öffentlichen Netzen aktuell auf Basis H.323 implementiert ist, sind einige Signalisierungs-Gateways für eine Konvertierung zwischen SIP und H.323 verfügbar (siehe Abbildung 3.14). Dies funktioniert normalerweise für die Basis-Funktionen wie Rufauf- und –abbau, macht aber noch Probleme bei Einzelfunktionen, z.B. wenn bei Zustands-Leveln die Skalierungen nicht übereinstimmen oder bei Anrufzulassung, wenn inkompatible Gruppenkonzepte vorliegen.

Inzwischen gibt es auch Standard-Ansätze für Signalisierungs-Konvertierung. Obwohl sie unvollständig sind und einige Teilfunktionen proprietär bleiben werden, ist dies der richtige Weg:

SIP Request Message	
Request Message Zeile	Beschreibung
INVITE sip: bob@acme.com SIP/2.0	Request-Zeile: Method-Typ, Request URI (SIP Adresse des gerufenen Teilnehmers), SIP Version.
Via: SIP/2.0/UDP	Adresse des letzten Hops.
alice_ws.ubn.de	
From: Alice A. <sip:alice@ubn.de>	Benutzer, der den Request gestellt hat.
To: Bob B. <sip:bob@acme.com>	Ausgesprochener Benutzer, wie ursprünglich spezifiziert.
Call-ID: 2388990012@alice_ws.ubn.de	Global eindeutige ID dieses Anrufs.
Cseq: 1 INVITE	Kommando Sequenz, identifiziert Transaktion.
Subject: Lunch today.	Anruf-Thema und/oder Art.
Content-Type: application/SDP	Body-Typ - in diesem Fall SDP.
Content-Length: 182	Anzahl Bytes im Body.
	Leerzeile, markiert Ende des SIP Headers und Beginn des Bodys.
v=0	SDP Version.
o=Alice 53655765 2353687637 IN IP4 128.3.4.5	Owner/Creator und Session Identifier, Session Version, Adress-Typ und Adresse.
s=Call from Alice.	Session-Thema.
c=IN IP4 allice_ws.ubn.de	Verbindungs-Information.
M=audio 3456 RTP/AVP 0 3 4 5	Media Beschreibung: Typ, Port, mögliche Formate, die der Anrufer empfangen und senden kann.

Abbildung 3.12: INVITE Request bei SIP

SIP Response Message	
Response Message Zeile	Beschreibung
SIP/2.0 200 OK	Status-Zeile: SIP Version, Response Code, Ursachenbeschreibung.
Via: SIP/2.0/UDP alice_ws.ubn.de	Kopiert aus Request.
From: Alice A. <sip:alice@ubn.de>	Kopiert aus Request.
To: Bob B. <sip:bob@acme.com>; tag=17462311	Kopiert aus Request. Enthält eindeutigen Tag, um den Anruf zu identifizieren.
Call-ID: 2388990012@alice_ws.ubn.de	Kopiert aus Request.
Cseq: 1 INVITE	Kopiert aus Request.
Content-Length: 200	
	Leerzeile, markiert Ende des SIP Headers und Beginn des Bodys.
v=0	SDP Version.
o=Bob 4858949 4858949 IN IP4 192.1.2.3	Owner/Creator und Session Identifier, Session Version, Adress-Typ und Adresse.
	Leerzeile, markiert Ende des SIP Headers und Beginn des Bodys.
s=Lunch	Session-Thema.
c=IN IP4 machine1.acme.com	Verbindungs-Information.
m=audio 5004 RTP/AVP 0 3	Beschreibung der Media Streams, die der Anruf-Empfänger akzeptieren kann.

Abbildung 3.13: INVITE Response bei SIP

- RFC 3398 definiert ein Mapping zwischen ISUP und SIP, um SIP/ISDN Integration zu erreichen
- Draft-ietf-sipping-qsig2sip-02 beschäftigt sich mit dem Mapping zwischen Q.SIG und SIP

MGCP und MeGaCo sind eher komplementär zu SIP zu sehen, da sie keine vollständige Signalisierungs-Lösung darstellen. MGCP und MeGaCo sind in der Architektur unterhalb von SIP anzusiedeln und können durch SIP kontrolliert werden.

Für IM hat sich zwar die Mehrheit der Provider auf SIP geeinigt und phasen ihre proprietären Protokolle aus, aber die IETF standardisiert zwei IM Protokolle: das SIP-basierte SIMPLE und das XML-basierte Jabber, ein Standard der Open-Source-Gemeinde. Beide bieten ähnliche Funktionalität und es gibt Entwürfe, SIP zum Aufbau von Jabber Sessions zu nutzen.

3.6 Aktuelle Weiterentwicklungen der Standards

Die Menge der SIP Spezifikationen ist inzwischen auf knapp 50 RFC's angewachsen, darunter auch Dokumente wie

- „Best Current Practice" für 3rd Party Rufkontrolle (RFC 3725, BCP0085)
- Authentifizierung Autorisierung, Accounting (RFC 3702, RFC 3329, RFC 3323-3325, RFC 3313)
- Erweiterung für Instant Messaging (RFC 3428)
- Mapping zwischen ISUP und SIP für Overlap Dialing (RFC 3578)
- Ressourcen Priorisierung (RFC 3487)
- Kompression für SIP (RFC 3486)
- Header-Erweiterungen für 3GPP (RFC 3455)
- SIP für Telefone (SIP-T, RFC 3372, BCP0063)
- SIP und 3G Mobilfunk (Static Dictionary für Kompression RFC 3485, Kompression RFC 3320, Registrierung nicht-benachbarter Kontakte RFC 3327)
- Parameter-Änderung bei laufender Session (RFC 3311)
- Benachrichtigung über spezielle Events (Register, Subscribe, Notify; RFC 3265)

Weitere Funktionen und Dienste erarbeiten die IETF Arbeitsgruppen SIP, SIPPING (Session Initiation Proposal INvestiGation) und SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions); hierzu gehören

- Nutzung von E.164 Nummern
- Rufkontrolle durch Dritte, Multi-Party
- SCTP (Stream Control Transmission Protocol als Transport Layer) bei großen Datenvolumen
- Weitere Leistungsmerkmale wie Konferenzschaltung, Message Waiting Indication, Transfer
- Vorankündigung (z.B. vor Konferenzschaltungen) und Wählton-Generierung
- Anrufpräferenzen

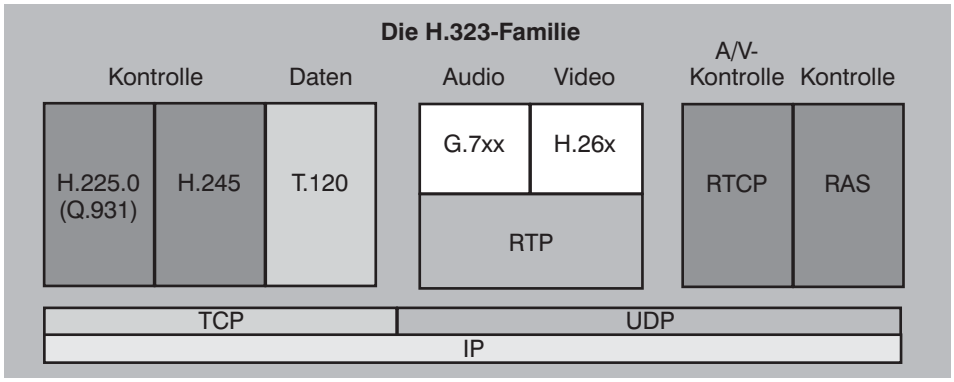


Abbildung 3.15: Die H.323 Protokollsuite

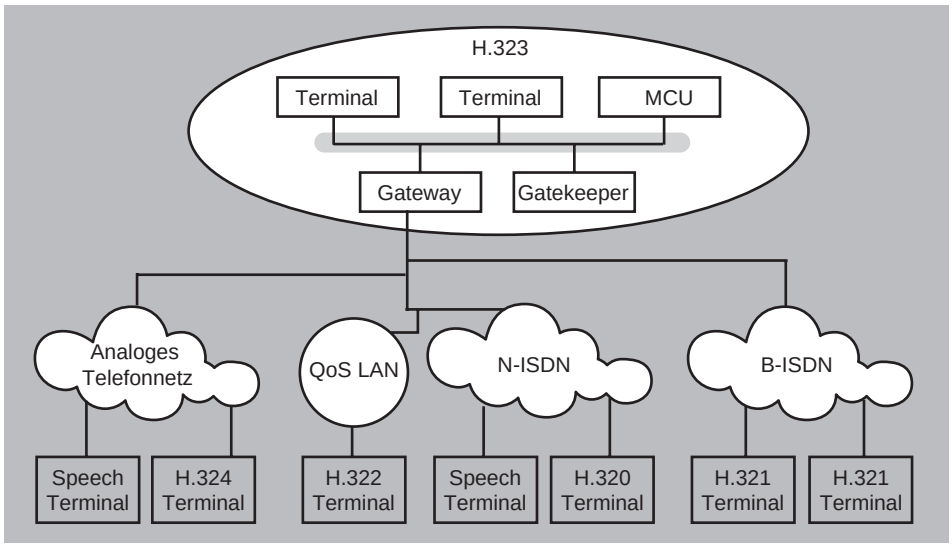


Abbildung 3.17: Übersicht einer H.323 Architektur und Konfiguration

Signaling		
H.323 Protocol Suite		
H.323 V2	ITU	Paket-basierende Multimedia-Kommunikations-Systeme
H.225.0	ITU	Call-Signalisierungs-Protokolle und Media-Stream Paketierung für Paket-basierte Multimedia (enthält Q.931 und RAS)
H.225.0 Annex G	ITU	Gatekeeper-zu-Gatekeeper (Inter-Domain) Kommunikation
H.245	ITU	Kontroll Protokoll für Multimedia Kommunikation
H.235	ITU	Sicherheit und Verschlüsselung für H-Serie Multimedia Terminals
H.450.x	ITU	Call Hold, Call Park und Pickup, Message Waiting Indication, Call Waiting, Name Identification, Call Completion, Call Offer, Call Intrusion, Additional Common Information Network Services)
H.323 Annex D	ITU	Echtzeit-Fax unter Nutzung von T.38
H.323 Annex E	ITU	Verbindungsaufbau über UDP
H.323 Annex F	ITU	Single-use Gerät
T.38	ITU	Prozeduren für Echtzeit Gruppe 3 Faksimilie-Kommunikation über IP Netzwerke
T.120 Serie	ITU	Daten-Protokolle für Multimedia-Konferenzen

Abbildung 3.18: H.323-Protokollsuite

- Notruf-Dienste
- SIP / QSIG Interworking

Weitere Arbeiten beschäftigen sich mit den Themen Sicherheit, Priorisierung, Kompression, Transcoding und Überlaststeuerung.

3.7 EXKURS: ITU-Standard H.323

Für Voice-over-IP gilt seit circa 1996 die H.323-Suite der ITU-T, die als Zielsetzung die herstellerübergreifende, kompatible Übertragung von Audio, Video und Daten über IP-Netze hat, wobei IP-Netze als Netze ohne Quality-of-Service betrachtet werden. H.323 ist ein Standardansatz, dessen Hauptanwendungsbereiche die Signalisierung und Sessionsteuerung, also Kontrollfunktionen sowie die Definition von Endgeräteschnittstellen sind. H.323 ist die Oberbezeichnung einer Reihe von Spezifikationen für Multimedia-Kommunikation über LANs, die keine garantierte Dienstgüte zur Verfügung stellen. Hierzu gehören theoretisch Ethernet, Token Ring und FDDI; Hardware-Telefone sind jedoch ausschließlich mit Ethernetanschluss erhältlich. Die Zusammensetzung des H.323-Stacks sowie die genutzten Transportprotokolle zeigen Abbildung 3.15 und Abbildung 3.16
Die in H.323 definierten Komponenten sind User Terminals, Gatekeeper (GK), Multipoint Control Units (MCU) und Gateways zur Verbindung in andere Welten, insbesondere zum PSTN-Netz (siehe Abbildung 3.17). Terminals sind Multimedia-, Video- oder Audio-Endgeräte. Gatekeeper sind die Kontrollinstanzen, bei denen sich Terminals anmelden und autorisiert werden müssen. Der GK erledigt außerdem Dinge wie Adressresolution, Bandbreitenmanagement, Verwaltung der Verzeichnisdienste. MCUs leisten Chairman-Funktionen, wie beispielsweise die Konferenzsteuerung mit Zuschalten, Ausloggen, Steuerung der Redeberechtigung und Kameraausrichtung für Telefon- und Videokonferenzen, wobei Konferenzen auch ohne eine solche Steuerung stattfinden können. Terminals können rechnerbasiert (Softphone) oder standalo-

Transport		
RTP (RFC 1889)	IETF	RTP; Real-Time Transport Protocol
RTCP (RFC 1889)	IETF	RTCP; Real-Time Transport Control Protocol
RTSP (RFC 2326)	IETF	RTSP; Real-Time Streaming Protocol

Abbildung 3.16: Transport Protokolle

ne (Hardphone) PCs, PCs mit Handset oder Headset, Hardware-Telefone, Videokameras und vieles mehr sein. Verbindungen sind als Punkt-zu-Punkt- oder als Multipunkt-Verbindungen (letzteren Fall mit Multicasts) betreibbar. Über die Gateway-Funktion sind auch andere Netze als LANs in die Multimedia-Kommunikation integrierbar wie ISDN (H.320), ATM (H.321) oder PSTN (H.324).

Unter H.323 werden Funktionen wie paketbasierte Multimedia-Kommunikation, Signalisierung, Kommunikation zwischen Gatekeepern, Verbindungskontrolle, Sicherheit und Verschlüsselung, Zusatzdienste vom Fax bis hin zu verteilten Applikationen spezifiziert wie in Abbildung 3.18 dargestellt. Inzwischen ist H.323 Version 3 verabschiedet, die meisten Hersteller unterstützen jedoch erst H.323v2. Da viele Funktionen optional und in Einzelstandards definiert sind, beschränkt sich die so genannte Standardkompatibilität teilweise auf die Basisfunktionen wählen, abnehmen, reden, auflegen. Da die ITU-Standardisierung ein zäher Prozess ist, wurden bisher lediglich folgende Zusatzfunktionen definiert: Rufweiterleitung, Rufumleitung, Halten, Parken, Wiederaufnehmen, Warteschlange, Nachrichtenanzeige, Namensanzeige, Einschalten in einen Call, zusätzliche allgemeine Netzinformationsdienste.

Allen Standards ist deutlich die Nähe zum etablierten TK-Netz bzw. Sprachübermittlungsdiensten anzumerken.

3.8 EXKURS: MeGaCo / MGCP

MGCP (RFC 2705) und seine Erweiterung MeGaCo (RFC 3015 / ITU H.248; RFC 3054) wurden von der Telco Seite entwickelt, um eine Integration von SS7 mit VoIP zu erreichen, weil die H.232 Initiative aus der LAN Welt kam und Skalierungs-Probleme mit sich brachte, da die dort definierte Architektur inkompatibel zur Welt der Telekom Dienste war, mit einer Vielzahl an Gateways und dem SS7 kämpfte. Um diese Probleme zu bewältigen, weitete die MeGaCo Initiative die Gatekeeper Funktion aus und lagerte die Signalisierungs-Kontrolle vom Gateway auf einen „Gateway-Controller“ oder „Softswitch“ aus (siehe). Damit wurde der Gatekeeper eigentlich in seine SS7-Äquivalente „zerlegt“. MGCP und MeGaCo sind Protokolle, die zwischen Gateway und Softswitch / Controller laufen, um die Kontrolle des Gateway durch den Softswitch / Controller zu erlauben.

Der Gateway Controller als zentrale Intelligenz entspricht praktisch den „Central Offices“ der klassischen PSTN-Welt. Der MeGaCo Ansatz bildet eigentlich die klassische PSTN-Architektur auf IP ab und steht damit im Gegensatz zu dem verteilten Modell verteilter Dienste von SIP und dem Internet.

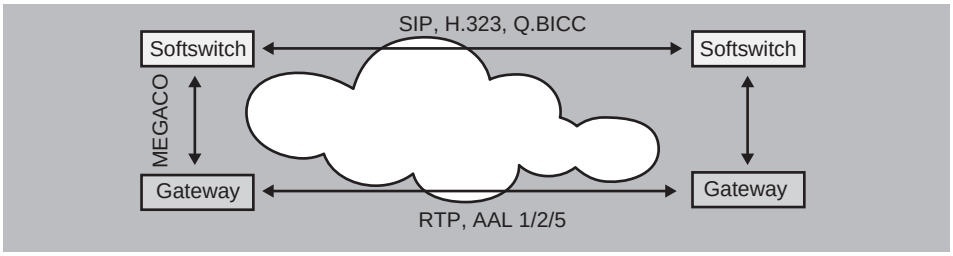


Abbildung 3.19:MeGaCo / MGCP Architektur

Vergleich von SIP und H.323	
SIP	H.323
Horizontale Struktur vorausgesetzt	Vertikale Struktur vorausgesetzt
Für WAN und Carrier Lösungen designed	Für LAN und Videoconferencing designed
Charakteristiken	
Toolkit Charakter; Nutzt etablierte IETF Elemente (URL‘s, MIME, DNS)	Spezifiziert alle Details (Codec, Media, Protokoll-Aktionen)
Verfügbarkeitsprobleme muss das unterliegende Netzwerk regeln	aktive Sockets nur bei Nutzung von Capabilities
SIP Nachrichten haben Textformat (wie Web und E-Mail)	H.323 Nachrichten haben ASN.1 Binärformat
Ermöglicht Standard-basierte Erweiterungen, um non-Standard Elemente zu realisieren	Ermöglicht Erweiterungen über „vendor-specific“ Funktionen
Hierarchische Adressierung im URL Stil, skalierbar	Adressierung mit limitierter Skalierung
Prioritätsfeld im Header	keine Prioritätensteuerung
Schlechte Spezifikation, wie ein Gatekeeper gefunden wird	Gute Spezifikation, wie ein Gatekeeper gefunden wird
Einfache Signalisierung, entsprechend niedriges Delay	Komplexe Signalisierung (Delay bis zu 7 oder 8 Sek.)
Dienste	
Standard IP Centrex	Standard IP Centrex
nein	Konferenzsteuerung
Fork von Anrufen, Multicast Signalisierung	aktuell nicht möglich
Benutzerprofile	nein
Unified Messaging	nein
Präsenzmanagement (IM, Presence)	nein
Beliebige Multimedia Dienste integrierbar	nur Voice und Videoconferencing bisher definiert
Status	
Neuer Standard, viele Ankündigungen	Weite Verbreitung
hohe Entwicklungs-Aktivitäten	Entwicklung vielfach eingefroren
wenige Produkte	viele existierende Produkte

Abbildung 3.20: Vergleich von SIP und H.323

3.9 SIP versus H.323 und MeGaCo

Gegenüberstellungen von SIP und H.323 sowie SIP und MeGaCo sind als Vergleichstabellen in Abbildung 3.20 und zusammengefasst. SIP gewinnt zwar immer

Vergleich von SIP und MeGaCo / MCGP	
SIP	MeGaCo / MGCP
Peer-to-Peer Signalisierungs-Protokoll	Kontroll-Protokoll, kann genutzt werden, um Dienste über ein Netzwerk zu vermitteln
Protokoll zum Session-Aufbau, erforderlich zwischen verschiedenen Softswitches	Zur internen Kontrolle von VoIP Gateways genutzt (Media-Gateways, Signalisierungs-Gateways, Transcoding-Gateways)
Prinzip: Einfach, wenig kontrolliert und horizontal	Prinzip: Zentralisiert, kontrolliert und vertikal
Client-Server Architektur	Master-Slave Architektur
„Reine“ IP Lösung	Interims-Lösung für Koexistenz von VoIP und PSTN
	macht PSTN IP-netzfähig
Horizontale Architektur, die Internet-Elemente nutzt	Abbildung der Singnalisierung und Kontrolll-Architektur von IN
Intelligente Clients / Endgeräte	Unintelligente Endgeräte
Trennt die Signalisierung vom unterliegenden Netzwerk	Setzt geeignete Hardware voraus

Abbildung 3.21: Vergleich von SIP und MeGaCo

mehr an Bedeutung, ist aber noch eine junge Technik und wird noch für fünf bis zehn Jahre mit H.323 koexistieren. Wie schnell sich SIP durchsetzt, wird letztlich der Markt entscheiden.

Fazit

SIP bildet die Basis für unsere zukünftige Kommunikation. Es ist einfach, stabil und flexibel. Insbesondere integriert es völlig verschiedene Kommunikationsdienste von der Sprache über Video zur Kollaboration.

SIP ist erweiterbar. Auf der einen Seite ist dies positiv, gestattet es doch den Herstellern, fehlende Leistungsmerkmale individuell zu entwickeln. Auf der anderen Seite wird diese Erweiterbarkeit dazu führen, dass Herstellerspezifische Lösungen entstehen. Die genormte SIP-Basis wird dann den gemeinsamen Nenner bilden.

Fortsetzung im nächsten Insider.

Wir haben auf unserem Web-Server ein Abkürzungs- und Literaturverzeichnis zu diesem Artikel hinterlegt, den Sie sich bei Interesse über diesen Link herunterladen können.
Abkürzungsverzeichnis

Sitemap für die Nach-Lese (nich ganz ernst gemeint)

DS-0 Dumping Signal für 0 Bock

H.323 Hexcodierung für die Anwahl einer internationalen Partnervermittlung auf Basis IP Telefonie

H.325 Hexcodierung für die Anwahl einer internationalen Partnervermittlung auf Basis IP Telefonie mit Anonymitäts-Zusicherung für privilegierte Kunden

IN In Need: zukünftig weltweites SOS Signal, über Web sendbar, für in Not geratenen VoIPer, dessen implantierter Headset Chip aufgrund verstärkter Denktätigkeit abgeraucht ist

MGCP Motivation Gateway-Operator Call Procedure: psychologen gesteuertes Motivationstherapie Gespräch (über Internet) für Gateway-Betreiber, die durch ständige Ausfälle gefrustet sind

RAS Reboot A Server: Protokoll zum intervallgetriggerten vorbeugenden Neustart von VoIP Gatekeepern, die auf Basis NT Server betrieben werden, erhöht die Verfügbarkeit mit einer Wahrscheinlichkeit von 30%, da Public Domain Code von Microsoft SIP Abkürzung für die Sippe der IP Telefonierer

SS7 Session Start 7: Selbstvernichtungs-Skript für VoIP Protokollstack nach 7 Fehlversuchen; optional aktivierbar

VoIP Voll mit Ollen IP Paketen

CCNE

ComConsult Certified Network Engineer

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

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

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

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

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

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
05.07. - 09.07.04 in Aachen
08.11. - 12.11.04 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
10.05. - 14.05.04 in Aachen
06.09. - 10.09.04 in Aachen
22.11. - 26.11.04 in Aachen

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

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

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

CCSE

ComConsult Certified Security Expert

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

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

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

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

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

Impressum

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

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

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

Chefredakteur: Dr. Jürgen Suppan

Erscheinungweise: Monatlich, 12 Ausgaben im Jahr

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen