



Untersuchung und Bewertung von VoIP-Diensten im Gigabit-Wissenschaftsnetz

Christian Grimm¹, Steffen Heinze¹, Eduard Siemens¹, Stefan Piger¹ und Sven Heese²

¹ Regionales Rechenzentrum für Niedersachsen (RRZN)
Universität Hannover
Schloßwender Straße 5, D-30159 Hannover
{grimm,heinze,siemens,piger}@rrzn.uni-hannover.de

² T-Systems International GmbH
Hans-Böckler-Allee 1, D-30173 Hannover
sven.heese@t-systems.com

Zusammenfassung: Der Beitrag befasst sich mit einem möglichen Betriebsmodell für den Einsatz von VoIP im DFN-Umfeld. Im Rahmen eines Projekts der Partner T-Systems, Cisco, DFN-Verein und Universität Hannover/RRZN wird untersucht, wie ein von einem externen Dienstleister betriebener VoIP-Dienst – hier von T-Systems angeboten und mit Komponenten von Cisco realisiert – umgesetzt werden kann. Neben strategischen Aspekten, die allgemein den aktuellen Wandel von der klassischen zur IP-Telefonie darstellen, werden hierbei auch spezifische Parameter und Anforderungen betrachtet, die bei einer Migration zu VoIP zu beachten sind.



1 Einleitung

Ziel des Projektes *Untersuchung und Bewertung von VoIP-Diensten im Gigabit-Wissenschaftsnetz* ist es, aus einem Testbetrieb heraus die Parameter und Anforderungen für den regulären Betrieb eines externen IP-Telefoniedienstes für Mitgliedseinrichtungen des DFN-Vereins festzulegen. In Zusammenarbeit der Projektpartner T-Systems, Cisco, DFN-Verein und Universität Hannover/RRZN wird untersucht, wie weit sich die Anforderungen mit existierenden Produkten umsetzen lassen und welche weiteren Dienstmerkmale für einen Regelbetrieb im Wissenschafts- und Forschungsumfeld erforderlich sind. Anschließend wird geprüft, welche der fehlenden Merkmale bereits während der Laufzeit des Pilotbetriebs realisiert werden können und welche erst in einem späteren Regelbetrieb bereitgestellt werden.

2 Strategische Aspekte

2.1 Wandel von der klassischen zur IP-Telefonie

Derzeit lassen sich deutliche Anzeichen für einen Wechsel von der klassischen Telefonie zur IP-Telefonie identifizieren:

- Entwicklungsvorhaben für die klassische Telefonie finden kaum noch statt. Diese Technologie lässt kein Wachstum mehr erwarten. Alle Hersteller klassischer TK-Anlagen bieten inzwischen mehr oder weniger proprietäre Migrationslösungen zur IP-Telefonie an.





- Das Sprachaufkommen verringert sich stetig im Vergleich zum Datenaufkommen, sowohl in privaten Netzen (Unternehmensnetze) als auch in öffentlichen Netzen (Providernetze). Aus wirtschaftlichen Erwägungen werden daher sowohl von Unternehmen als auch von Netzbetreibern keine getrennten Netze mehr für Sprache und Daten realisiert. Der relativ geringer werdende Anteil an Sprachkommunikation wird vielmehr über die ohnehin breitbandigen Datennetze übertragen.

Aufgrund der hohen Qualitätsanforderungen von Sprachanwendungen beschränkt sich der Einsatz der IP-Telefonie zunächst auf breitbandige Netze. Hierzu zählen *local area networks* (LANs) sowie breitbandige *wide area networks* (WANs) wie z. B. das deutsche Wissenschaftsnetz G-WiN.

2.2 Einflussgrößen

Die Geschwindigkeit der Migration zur IP-Telefonie wird maßgeblich von folgenden Faktoren beeinflusst:

- durch die Gesamtkosten im Vergleich zur klassischen Telefonie, z. B. ausgedrückt durch die so genannten Pro-Port-Kosten,
- durch den Mehrwert, der aus dem Grad des Zusammenwachsens von Daten- und Sprachkommunikation neue Applikationen und Geschäftsmodelle ermöglicht,
- durch Lösungsmodelle, die einer Einrichtung oder einem Unternehmen die Migration zur IP-Telefonie erleichtern.

Die Frage der Migration zur IP-Telefonie stellt sich früher oder später für jede Mitgliedseinrichtung im DFN-Verein. Die dabei zu lösenden Aufgaben sind vielschichtig und teilweise schwierig. Es liegt im Vereinsinteresse, diese Fragestellungen zentral aufzuarbeiten und den Mitgliedseinrichtungen rechtzeitig Hilfen und ggf. Lösungen anzubieten. Dies ist das Ziel des durchgeführten Projektes.

2.3 Vorteile durch den Einsatz von VoIP

Der Aufbau und Betrieb nur noch eines universellen Netzes für Daten und Sprache ist ein offensichtlicher Vorteil der IP-Telefonie. Ein weiterer Vorteil ist die Nutzung herstellerübergreifender Standards. Bei den Nebenstellenanlagen grenzen sich die Hersteller durch den Einsatz proprietärer Protokolle und Endgeräte voneinander ab. Protokoll-Familien wie H.323 oder das Session Initiation Protocol (SIP) schaffen hierfür herstellerübergreifende Standards – sofern sie nicht ebenfalls durch proprietäre Erweiterungen ergänzt werden.

Wichtige Potentiale der IP-Telefonie stecken im Mehrwert. Durch das Zusammenfügen der Daten- und Sprachkommunikation entstehen neue Dienste, wie

- Internet-weite Erreichbarkeit des Teilnehmers unter „seiner“ Rufnummer (Erhöhung der Mobilität)
- Internet-Anwendungen mit integriertem Sprachdialog (Erhöhung der Mediendurchdringung)
- Zusammenführung aller Nachrichten in einem Medium (Unified Messaging)



- Integration von Telefonie und Datenanwendungen (CTI, Computer Telephony Integration)

Trotz der Vorteile und Potentiale wird VoIP vom Markt aber immer noch zögerlich angenommen. Ursächlich hierfür sind u. a.:

1. Der Technologiewechsel von einem bestehenden, sehr zuverlässigen, verbindungsorientiertem System zu den verbindungslosen IP-Netzen im LAN, MAN oder WAN, welche als grundsätzlich unzuverlässig betrachtet werden müssen. Einbußen an Zuverlässigkeit und Verfügbarkeit der Telefonie werden nicht bzw. nur sehr begrenzt in einem Rahmen akzeptiert, in dem bei gleichem Preisniveau ein erkennbarer und interessierender Mehrwert angeboten wird.
2. Die ISDN-Infrastrukturen im Bereich der Unternehmen (TK-Anlagensysteme) sowie der Netzanbieter (SDH-Netze) haben hohe Standzeiten. Ein Technologiewechsel ist daher ein mehrjähriger Prozess, der eine zusätzliche Belastung bedeutet, sowohl in finanzieller als auch in personeller Hinsicht.
3. Gerade im Hochschulbereich sind gewachsene Strukturen mit getrennten Verantwortlichkeiten für den Fernsprech- und den Datendienst weit verbreitet. Es ist zwar vielerorts gelungen, universelle Netzinfrastrukturen für den Fernsprech- und Datendienst aufzubauen, die Netze sind aber weiterhin physisch getrennt. Es fehlt häufig ein Konzept, unter wessen Verantwortlichkeit die IP-Telefonie als Standard-Dienstleistung in der Hochschule angeboten werden soll.
4. Es gibt etliche Kostenbetrachtungen zu dem Einsatz und Betrieb klassischer Telefonanlagen im Vergleich zur IP-Telefonie. Bei allen, auch den unterschiedlichsten Kalkulationen gilt jedoch: Der Einsatz der IP-Telefonie erfordert zusätzlichen Personalaufwand, der beim Ansatz einer vergleichbaren Verfügbarkeit zur klassischen Telefonie nicht „nebenher“ erledigt werden kann. Weiterhin müssen zentrale Netzkomponenten für die IP-Telefonie beschafft und gepflegt werden. Da der Technologiewechsel sich langsam vollzieht (siehe 2.) und die klassische Telefonie nicht sofort durch die IP-Telefonie verdrängt wird, ist häufig ein mehrjähriger Parallelbetrieb erforderlich. Dadurch entstehen in jedem Fall zusätzliche Kosten.

2.4 Umstieg von der klassischen Telefonie auf IP-Telefonie

Für jede Einrichtung stellt sich eine wichtige Frage: Wann soll der Einstieg in die IP-Telefonie erfolgen? Häufig steht diese Entscheidung eng im Zusammenhang mit der Erneuerung oder auch dem Ausbau einer vorhandenen TK-Anlage. Die Entscheidungsträger müssen sich dabei bewusst sein, dass sie sich mit einer Entscheidung zu Gunsten der klassischen Telefonie erneut für viele Jahre an einen Hersteller binden.

Für die Mitgliedseinrichtungen im DFN-Verein bestehen hervorragende Voraussetzungen, den Einstieg in die IP-Telefonie zu erproben. Seit Mitte 2003 ist im G-WiN ein experimenteller IP-Telefonie-Verbund in Betrieb, den alle Mitgliedseinrichtungen nutzen können (s. Interessensarbeitskreis „VoIP-Verbund“ in [HOO+03]). Praktische Erfahrungen haben gezeigt, dass das G-WiN und die heute üblichen LAN-Infrastrukturen mit *Fast Ethernet* und *switched networks* eine zumeist ausreichende, bei entsprechender Dimensionierung



annähernd echtzeitfähige Infrastruktur zur Sprachkommunikation bereitstellen. Für einen Technologiewechsel zur IP-Telefonie verbleiben damit zwei wesentliche Fragestellungen:

1. Wie kann das Investitionsproblem zufrieden stellend gelöst werden?
2. Wie soll der Dienst in geeigneter Weise erbracht werden?

2.5 Das Betreibermodell

Die Projektpartner haben im Vorfeld des Projektes einen intensiven Erfahrungsaustausch zur IP-Telefonie betrieben, bei dem u. a. auch die beiden oben aufgeführten Fragen beraten wurden. Die Erkenntnisse lassen sich so zusammenfassen, dass ein externes Betreibermodell die genannten Randbedingungen vermutlich sehr gut erfüllen dürfte:

- Die Vollkosten für die IP-Telefonie sind wesentlich durch den Personalaufwand für Konfiguration und Betrieb und weiterhin durch die zentralen Netzkomponenten, wie z. B. Callmanager oder VoIP-Gateways, geprägt. Für kleinere Organisationseinheiten mit geringen Portzahlen ergibt sich dabei für VoIP ein vergleichsweise hoher Portpreis, bei großen Portzahlen sinkt der Portpreis entsprechend. Mittlerweile existieren etliche Untersuchungen zu den Einsparpotentialen mit VoIP. Eine Kalkulation der Universität Hannover ist dabei sehr konservativ: erst bei Portzahlen ab ca. 2.000 Anschlüssen wird der *break even point* im Vergleich zu den Kosten der klassischen Telefonie erreicht. Eine Untersuchung der DeTelLine kommt zu dem Ergebnis, dass die Kosten für die IP-Telefonie nur halb so hoch sind wie die der klassischen TK-Anlagen-Technik. In jedem Fall lassen sich durch Bündelung des Personalaufwandes und der Netzkomponenten Einsparungen erzielen. Ein Betreibermodell, das durch ein entsprechendes Dienstleistungsangebot die Nachfrage bündelt, verspricht daher besonders wirtschaftliche Vorteile (Skaleneffekt). Ein typisches Beispiel hierzu ist ein Dienstleistungsangebot für die Mitglieder des DFN-Vereins im Verbund des Wissenschaftsnetzes.
- VoIP ist (noch) keine „plug & play“-Lösung und erreicht die hohe Verfügbarkeit klassischer TK-Anlagen nur durch zusätzlichen Aufwand (redundante Server, erfahrenes Betriebspersonal, proaktive Wartungen). Die Einführung von VoIP erfordert geschultes Personal, das in kleinen und mittleren Organisationseinheiten tendenziell schwer bereitzustellen ist. Da Betrieb und Service in dem hier untersuchten Modell ausgelagert werden, ist der Personalaufwand für die F&E-Einrichtungen gering. Den Einrichtungen wird somit eine sanfte Migration „Schritt für Schritt“ ermöglicht, ohne besonderen zusätzlichen Investitions- und Betriebsaufwand.

3 Ziel des Projektes

3.1 Praktische Erprobung

In dem Projekt soll festgestellt werden, wie weit sich die in Kapitel 2.5 genannte Vorstellung mit existierenden Produkten umsetzen lässt und welche Dienstmerkmale für einen Regelbetrieb im geplanten Umfeld erforderlich sind. Das Projekt soll weiterhin dazu dienen, die Parameter und Anforderungen eines Dienstes für die IP-Telefonie zu erkennen, praktisch zu erproben und für ein mögliches Dienstangebot festzulegen.



Für die praktische Erprobung muss zunächst die Konfiguration der Testumgebung mit der erforderlichen Integration des IP-Netzes und der TK-Anlage der Einrichtung festgelegt werden. Neben den funktionalen Tests dieser Konfiguration ist eine Reihe weiterer Fragenkomplexe zu bearbeiten, die für ein Dienstleistungsmodell wichtig sind. Hierzu gehören z. B. der Einsatz von Teamanlagen, der Aufbau von Verzeichnisdiensten zur Unterstützung zentraler Vermittlungs- und Auskunftsplätze, die Abrechnungsproblematik (von den Logdaten bis zum Gebühreneinzug) und Maßnahmenkataloge zu Fragen der Verfügbarkeit und Sicherheit.

4 Konfiguration und Erprobung der Testumgebung

Seit 2001 wird am RRZN eine VoIP-Installation aus ca. 100 IP-Telefonen mit Komponenten von Cisco betrieben. Das hierfür eingerichtete VoIP-VLAN ist mit redundanten Callmanagern, PIX Firewalls und VoIP-Gateways ausgestattet (Abb. 1 unten links). Eine Anforderung an das Projekt war, dass diese bestehende VoIP-Umgebung parallel zu der neu aufzubauenden betrieben werden konnte.

Gemäß dem Projektziel, IP-Telefonie als extern erbrachte Dienstleistung zu evaluieren, wurde die Testkonfiguration von Beginn an verteilt konzipiert. Die IP-Telefone und das VoIP-Gateway werden in einem eigenen Virtuellen LAN – im Folgenden VoIP-VLAN bezeichnet – der T-Systems über das Datennetz der Universität Hannover betrieben (Abb. 1 oben links). Die zentralen und wartungsintensiven Komponenten wie der Callmanager werden an einem räumlich entfernten Standort, der so genannten Service Area bei der T-Systems, administriert (Abb. 1 oben rechts).

Um einen möglichst breiten Überblick über die Akzeptanz in verschiedenartigen Umgebungen zu gewinnen, erstreckt sich das VoIP-VLAN der T-Systems über 50 Teilnehmer in mehreren Einrichtungen, die spezifische Anforderungen an ein Telefonie-System stellen und unterschiedliche Erfahrung mit IP-Telefonie besitzen. Durch die Beteiligung von Nutzern an der TU Braunschweig werden zusätzlich die Möglichkeiten zur Anbindung weiterer Einrichtungen mit eigenen Charakteristiken (z. B. Rufnummernplan, Gebührenmodell, Netzzugang) untersucht.

4.1 Nähere Erläuterung der Testumgebung

Der Cisco Callmanager befindet sich in der durch eine Firewall abgesicherten Service Area an einem Standort der T-Systems. Die Verbindung zwischen der Service Area und dem IP-Netz der Universität Hannover wird über das G-WiN hergestellt. Für das Break-Out wird ein VoIP-Gateway verwendet, das über einen Primärmultiplexanschluss mit dem öffentlichen Telefonnetz verbunden ist. Über das Merkmal „CLIP No Screening“ (CLIP: Calling Line Identification Presentation) wird sichergestellt, dass bei Anrufen nach extern die gesendete Nummer des Anrufers der über die TK-Anlage verwalteten Nummer des IP-Telefones entspricht. Dieses VoIP-Gateway stellt außerdem den DHCP-Service zur Vergabe der IP-Adressen für die IP-Telefone in Hannover bereit.

Das Konzept sah zunächst vor, auch das Break-In für Gespräche aus dem öffentlichen Telefonnetz über dieses Gateway zu ermöglichen. Da es sich bei dem für die VoIP-Umgebung

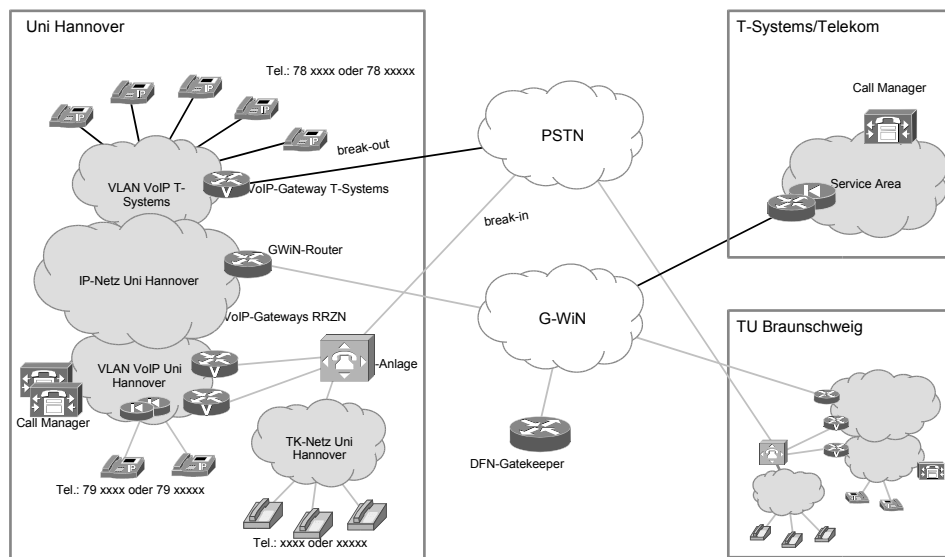


Abbildung 1: Konfiguration der Testumgebung

vergebenem Rufnummernblock allerdings um eine Untermenge des für die Universität Hannover maßgeblichen Bündels handelt, wären hierbei regulatorische und organisatorische Probleme aufgetaucht, die zu unverhältnismäßig hohem Mehraufwand geführt hätten. Aus diesen Gründen wird das Break-In nicht über dieses Gateway, sondern stattdessen über die TK-Anlage der Universität Hannover und die damit gekoppelten VoIP-Gateways des RRZN realisiert.

Gespräche zu Nebenstellenanschlüssen der Universität Hannover laufen über die VoIP-Gateways des RRZN zur TK-Anlage.

Die IP-Telefone an der TU Braunschweig sind ebenfalls über das G-WiN mit dem zentralen Callmanager in der Service Area verbunden. Auch bei diesen IP-Telefonen findet das Break-Out über das VoIP-Gateway in Hannover statt, um den Anschluß einer Einrichtung ohne eigenes Break-Out-Gateway auszutesten. Das Break-In aus dem öffentlichen Netz sowie die Verbindung zu Nebenstellenanschlüssen der TK-Anlage in Braunschweig wird über ein in Braunschweig vorhandenes Gateway realisiert, das mit der dortigen TK-Anlage verbunden ist.

Für Verbindungen zu IP-Telefonen in der bereits bestehenden VoIP-Umgebung des RRZN wurden über einen Intercluster Trunk die Callmanager von RRZN und T-Systems direkt miteinander gekoppelt.

Auf dem VoIP-Gateway der T-Systems in Hannover ist zusätzlich das SRST-Feature (Survivable Remote Site Telephony) eingerichtet. Dieses Feature übernimmt bei einem Ausfall des Callmanagers in der Service Area dessen grundsätzliche Funktionalität. Auch bei ei-

nem Ausfall der Verbindung zwischen VoIP-VLAN und der Service Area über das G-WiN wird diese Backup-Lösung aktiv.

4.2 Funktionale Tests

Im Anschluss an den Aufbau der Testumgebung wurden vor Beginn des Nutzerbetriebes zahlreiche Tests grundlegender und erweiterter Funktionen der VoIP-Umgebung durchgeführt. Der folgende Katalog liefert einen Überblick über die Vielzahl der getesteten Funktionen.

Grundfunktionen und Erreichbarkeit

- Telefonieren innerhalb der VoIP-Umgebung
- Telefonieren ins Amt
- Telefonieren zu Anschlüssen in TK-Nebenstellen der Universität Hannover
- Eingehende Gespräche aus dem Amt
- Eingehende Gespräche aus der TK-Anlage der Universität Hannover
- Erreichbarkeit von anderen Knoten der TK-Anlagen
- Telefonieren zwischen VoIP-Clustern (Intercluster Trunk)
- Erreichbarkeit über die TK-Querverbindungen (Behördennetz, TU Braunschweig)

Abrechnungssystem

- Trennung privater und geschäftlicher Telefonate (Anmerkung: mittels einer Auswahlkennziffer werden geschäftliche und private Telefonate für die Gebührenabrechnung getrennt.)
- Verarbeitung der Rechnungsdaten und Zustellung an den Verursacher

erweiterte Funktionen

- klassische Konferenz (auch mit externen Teilnehmern)
- Dial-In Konferenz (auch mit externen Teilnehmern)
- Gespräch halten
- Gesprächweiterleitung
- Rufumleitung

Übermittlung der Rufnummern

- korrekte Übermittlung der Rufnummern ins Amt
- korrekte Übermittlung der Rufnummern zu Nebenstellen der TK-Anlage sowie über die TK-Querverbindungen

Sprachqualität

- Sprachverständlichkeit
- Echoproblematik (intern, Amt, UH-Nebenstellen)
- Lautstärke (intern, Amt, UH-Nebenstellen)
- Silence Suppression



Endgeräte

- Ruftonkonfiguration/Ruftonlisten
- Einrichten und Nutzung eines Corporate Directory
- Speed Dials (Kurzwahltasten)
- Verwaltung persönlicher Verzeichnisse
- Konfiguration der Endgeräte über das Web-Interface des Call Managers
- Extension Mobility
- Einsatz von Softphones

4.3 Erste Empfehlungen zur Konfiguration für den Regelbetrieb

In Vorbereitung auf einen dauerhaften Regelbetrieb erscheint es sinnvoll, die technischen Gegebenheiten innerhalb der zu versorgenden Einrichtung genauestens zu erkunden (sogeannter Voice Ready Check). Zum anderen sollten die Erwartungen der Nutzer in Hinblick auf die Funktionalität einer neuen Telefonie-Lösung evaluiert werden und ein Abgleich mit dem technisch möglichen Rahmen der Ziellösung stattfinden.

Für das Datennetz kann ein geschwichtes 100 Mbit/s Ethernet-Netz als eine Mindestvoraussetzung für einen Sparchdienst guter Qualität genannt werden. Grundsätzlich besteht bei den folgenden Punkten Abstimmungsbedarf zwischen dem Dienstanbieter und den Einrichtungen bezüglich der gewünschten Einstellungen:

- Welcher Codec ist verfügbar und wird bei internen oder externen Gesprächen gewünscht? Da die geeignete Wahl des Codecs die Sprachqualität wesentlich beeinflusst, sollte hierbei auch die Auslegung des IP-Netzes berücksichtigt werden. Für interne Telefonate ist es empfehlenswert, bei entsprechender Kapazität des IP-Netzes den proprietären Wideband-Codec zu wählen, wodurch die Signalqualität verbessert wird.
- Da der Rufnummernplan für öffentliche Telefonie in Deutschland Rufnummern variabler Länge vorsieht, muss bezüglich des „Interdigit Timeout“, der die maximale Wartezeit zwischen zwei gewählten Ziffern bis zum Versuch der Anwahl der eingegebenen Nummer angibt, eine Einstellung als Kompromiss zwischen schnellem Wahlvorgang und guter Bedienbarkeit gefunden werden.
- Die Aktivierung bzw. Deaktivierung der „Anklopfen“-Funktion muß als Standardvorgabe oder für jeden Nutzer einzeln definiert werden
- Ein Default-Passwort für den Zugang zu den Administrationseinstellungen der Nutzer sollte eingerichtet werden
- Serverseitig sollten die gewünschten Lokalisierungen, Ruftonlisten, Belegungen der Softkeys, Music-On-Hold (Wartemusik) und verfügbaren IP-Phone-Services vorab nach den Erwartungen und Erfordernissen der Einrichtungen definiert und konfiguriert sein. Dies sollte bei einer Mehrmandantenlösung außerdem nach Mandanten getrennt möglich sein.

Neben den hier ausgeführten Erfahrungen aus dem Aufbau der Testumgebung erfordert die Planung einer entsprechenden VoIP-Umgebung für den Regelbetrieb besonders die in den Kapiteln 7, 8 und 9 aufgeführten Aspekte der Mandantenfähigkeit, der Verfügbarkeit und der Security.



5 Accounting und Billing

Accounting und Billing wird im Rahmen des Projekts flankierend betrachtet. Neben der Realisierung einer Lösung, mit der die anfallenden Gebühren für die Teilnehmer des Projektes abgerechnet werden, wird ein Anforderungskatalog für das Accounting und Billing in einem produktiven heterogenen Telefonie-Verbund erstellt.

5.1 Abrechnung für den Pilotbetrieb

Für die Durchführung des Projektes wird seitens T-Systems eine geeignete Software (AlwinPro der Firma Aurenz) bereitgestellt. Das Abrechnungssystem ist im VoIP-VLAN der T-Systems installiert und wird von der T-Systems administriert und gewartet. Nachfolgend wird das für den Pilotbetrieb implementierte Abrechnungsmodell dargestellt:

- Die T-Systems stellt dem RRZN monatlich eine Rechnung über sämtliche entgeltpflichtige Telefonate, die über den Anschluss der T-Systems ins öffentliche Netz geführt werden (break out). Dabei wird das Entgeltmodell für den DFN-Fernsprechdienst angewendet. Das RRZN überweist den Rechnungsbetrag nach Erhalt der Entgelte von den Teilnehmern auf das angegebene Konto.
- Die Erhebung der Verbindungsentgelte von den Teilnehmern basiert auf den Taktinformationen, die während der Verbindung von der DTAG im ISDN-Protokoll übertragen werden („Gebührentakte“, Advice of Charge – Charging Information During the Call, AOC-D). Dabei ist zu beachten, dass die Einrichtungen unterschiedliche Gebühren je Takt und sogar unterschiedliche Gebühren für dienstliche oder private Gespräche abrechnen können.
- Für jeden Teilnehmer wird jeweils eine Rechnung für private und dienstliche Telefonate inklusive Einzelbindungsnachweis erstellt. Diese Rechnungen dienen ausschließlich der Verrechnung der Verbindungsentgelte innerhalb der Einrichtung.
- Außerdem wird für jede teilnehmende Einrichtung eine Sammelrechnung erstellt, anhand welcher das RRZN die Telefongespräche mit der jeweiligen Einrichtung abrechnet.
- Zur Plausibilitätsprüfung wird eine Gesamtübersicht der Kosten für die Verbindungen erstellt.

Zu beachten ist, dass das Break-Out aller Teilnehmer in das öffentliche Netz über das VoIP-Gateway in Hannover erfolgt. Gespräche von Teilnehmern der TU Braunschweig in das Ortsnetz Braunschweig werden dadurch im öffentlichen Netz zu Ferngesprächen auf der Rechnung der T-Systems. Die Teilnehmer in Braunschweig sollen diese aber als Ortsgespräche in Rechnung gestellt bekommen. Für den Pilotbetrieb wird erwartet, dass der daraus resultierende Verlust durch den „Überschuss“ bei anderen Verbindungen ausgeglichen wird. Soll sich herausstellen, dass der Verlust nicht gedeckt wird, muss das Abrechnungsmodell nachträglich angepasst werden.

Im Verlauf des Piloten hat es sich gezeigt, dass die Sammlung der Gebühreninformationen für die Abrechnung der Teilnehmer sehr schwierig ist. Das VoIP-Gateway erhält zwar die Gebühreninformationen von der OVSt, ist aber nicht dafür geeignet, diese zu speichern oder weiter zu verarbeiten. Die eigentlichen Call Details werden im Callmanager



gesammelt, dieser erhält jedoch keine Informationen über die von der Vermittlungsstelle generierten Gebühreneinheiten.

Das verwendete Abrechnungssystem ermöglicht es, flexible Gebührenmodelle zu hinterlegen. Da die derzeit im Land Niedersachsen für den öffentlichen Bereich eingesetzten Abrechnungssysteme auf dem Taktmodell der DTAG basieren, musste bei der Implementierung des Abrechnungssystems ein daran angelehntes Modell synthetisch generiert werden. Bei zukünftigen Änderungen des Taktmodells der DTAG wäre eine manuelle Nachpflege des Tarifmodells notwendig.

Für die Rechnungsstellung wurde für jede teilnehmende Einrichtung eine Teilnehmergruppe gebildet. Die Abrechnung erfolgt dreistufig:

1. Als erstes wird eine Sammelrechnung über die Gesamtheit der geführten Telefonate aller Teilnehmer nach dem Gebührenmodell der jeweiligen Einrichtungen gebildet. Dies sind die vom RRZN zu erzielenden Einnahmen von den Teilnehmern. Diese müssen mit der Abrechnung seitens der T-Systems für das Bündel abgeglichen werden.
2. In der nächsten Stufe werden Sammelrechnungen für jede teilnehmende Einrichtung aufgestellt. Diese dienen der Abrechnung der Telefongebühren zwischen dem RRZN und den Einrichtungen.
3. In der dritten Stufe werden jeweils zwei Rechnungen pro Nutzer – für private und dienstliche Telefonate erstellt. Diese dienen für die einzelnen Nutzer zur Kontrolle bzw. für die Einrichtungen zur Abrechnung der privaten Telefonate mit den Teilnehmern.



5.2 Anforderungen an eine zukünftige Lösung

Für den Fall, dass für den Einsatz der IP-Telefonie eine teilnehmerbezogene, genaue Abrechnung erfolgen soll, wurden in dem Projekt Anforderungen an ein derartiges Abrechnungssystem zusammen getragen. Zielvorstellung ist dabei ein zentrales Abrechnungssystem, welches Call Detail Records von verschiedenen Telefonie-Systemen sammelt, auswertet und entsprechende Rechnungen erstellt. Nachfolgend werden die im Projekt herausgearbeiteten Anforderungen an ein derartiges Abrechnungssystem aufgelistet:

- Durch eine ein- oder zweistellige Titelkennzahl vor der Rufnummer wird der Zweck des eingeleiteten Gesprächs (z. B. dienstlich oder privat) festgelegt. An der Universität Hannover wird z. B. das Präfix „00“ für Privatgespräche, „01“ für Dienstgespräche verwendet. Grundsätzlich müssen auch die Präfixe „02“ bis „09“ unterstützt werden.
- Pro Teilnehmer soll jeweils eine Rechnung für jede verfügbare Titelkennzahl erstellt werden. Den Rechnungen sollen Einzelbindungsnachweise mit der Auflistung der vollen gewählten Rufnummer beigelegt sein. Optional muss eine Möglichkeit zur Kürzung der Rufnummer auf dem Einzelbindungsnachweis bestehen.
- Das System muss über eine flexible Teilnehmerverwaltung verfügen. Gruppenbildung von Teilnehmern und deren Zuordnung zu unterschiedlichen Kostenstellen soll möglich sein.
- Für den Import der Abrechnungsdaten z. B. in das SAP-System sollten entsprechende Schnittstellen bereitgestellt werden.





- Die Gesprächsdaten müssen vor der Rechnungserstellung einer Plausibilitätskontrolle unterzogen werden, um ungültige oder inkonsistente Daten auszufiltern.
- Das Inkasso für Privatgespräche wird über die Sekretariate bzw. Verwaltungen der Einrichtungen per Barzahlung abgewickelt. Für die Kontrolle der Zahlungseingänge müssen vom Billingsystem abteilungsbezogen so genannte „Buchungslisten“ generiert werden, in denen die zu zahlenden Entgelte je Teilnehmer aufgeführt sind.
- Die Definition der Lokalität, d. h. die Ausdehnung der Ortsnetz-Zone, ist unabhängig vom VoIP-Gateway, über das in das ISDN-Netz ausgestiegen wird.

6 Vermittlungsplatz-Dienste und Verzeichnis-Dienste

In Bereichen der klassischen Telefonie findet häufig ein Vermittlungsplatz-Dienst Anwendung. Dieser ist in der Regel auf ein Unternehmen bzw. eine Organisation beschränkt. Die Hauptaufgabe für einen Vermittlungsplatz-Dienst ist eine manuelle Vermittlung der Anrufer zum gewünschten bzw. zuständigen Mitarbeiter. Obwohl der Vermittlungs-Dienst historisch aus der Zeit der manuellen Vermittlung stammt, hat seine Bedeutung auch mit fortschreitender Entwicklung der Kommunikationstechnik nicht abgenommen. Vielmehr hat er sich mit der automatischen Verteilung von Rufen (Automatic Call Distribution, ACD) zu einem eigenständigen Zweig entwickelt.

Mit der Entwicklung der IP-Telefonie ist davon auszugehen, dass Vermittlungsvorgänge auch in heterogenen Umgebungen im Wesentlichen automatisch ablaufen werden. Ein moderner Vermittlungsplatz muss daher unterschiedliche Protokolle, insbesondere ISDN, SIP und H.323, beherrschen. Darüber hinaus wird die Kombination von Vermittlungsplatz-Diensten mit Verzeichnis-Diensten, wie sie in IP-Netzen durch LDAP und DNS bereits etabliert sind, eine wichtige Rolle spielen.

6.1 Verzeichnis-Dienste in IP-Netzen

6.1.1 LDAP

Das Lightweight Directory Access Protocol (LDAP) [HoMo02] bietet eine Basis für die strukturierte Speicherung und Verteilung von Daten. Die Daten werden in hierarchischen binären Baumstrukturen abgelegt, wobei die Verwaltung einzelner Zweige an unterschiedlichen Administratoren delegiert werden kann. Zurzeit werden LDAP-Verzeichnisse überwiegend für die Speicherung und Verwaltung von Gerätekonfigurationen sowie von Berechtigungen (z. B. beim Active Directory von Microsoft) verwendet.

6.1.2 DNS

Der Domain Name Service (DNS) hat sich seit ca. 20 Jahren als robuster und weltweit verfügbarer Service für die Abbildung von symbolischen Namen auf Geräteadressen (resp. IP-Adressen) bewährt. Durch die Erweiterungen *Service Records* und *Electronic Numbering* (ENUM) ist es heute sogar möglich, mit DNS verteilte hierarchische und ausfallsichere Verzeichnis-Dienste für multimediale Services, wie z. B. IP-Telefonie oder Videoconferencing, zu implementieren.





Mit Hilfe von Service Records [GVE00] [Mea02a] [Mea02d] [Mea02c] [Mea02d] können Abbildungen zwischen Diensten und zugehörigen Geräteadressen realisiert werden. So lässt sich zum Beispiel ein Server für den Dienst sip://auskunft@sip.rvs.uni-hannover.de definieren. Damit kann die Email-Adresse einer Person mit einem Kommunikationssystem, wie z. B. einem Festnetz-Telefon, einem IP-Telefon oder einem Videokonferenz-System verknüpft werden. Service Records ermöglichen es jedoch nicht, eine Verknüpfung zwischen einem Personennamen und zugeordneten Diensten zu realisieren.

Dienste werden im Internet in der Regel über weltweit eindeutige symbolische Namen adressiert. Herkömmliche Kommunikationssysteme werden über Zeichenketten adressiert, die typisch lediglich aus Ziffern (hier Telefonnummern) bestehen. Das Format dieser Zeichenketten wird z. B. im ITU-T Standard E.164 definiert. Aus historischen Gründen sowie aus Gründen der Interoperabilität mit den herkömmlichen Kommunikationssystemen werden bei dem Einsatz von IP-Telefonie und Videokonferenz-Systemen oft Rufnummern nach dem E.164-Schema verwendet. Eine Abbildung von Telefonnummern auf IP- bzw. Transportadressen mit Hilfe von DNS-Abfragen wird durch ENUM [FaMe04] festgelegt.

6.2 Vermittlungsplatz und Verzeichnis-Dienst

Zurzeit findet das ENUM-Modell bei der Zuordnung von Geräteadressen zu Telefonnummern zunehmend Verbreitung. Dies ist vor allem durch die Robustheit und Skalierbarkeit des DNS bei einer dynamischen Verwaltung von Telefonnummern begründet. Da ENUM aber keine direkte Zuordnung zwischen Personennamen und Service-URIs ermöglicht, wird für einen DFN-weiten Einsatz ein zusätzlicher Directory-Service benötigt. So ist es denkbar, dass im DFN-Umfeld ein einheitlicher LDAP-Service verwendet wird, in dem z. B. Email-Adressen und Telefonnummern Personen zugeordnet werden, die Auflösung von Email-Adressen bzw. Telefonnummern dabei aber dynamisch über einen ENUM-Service erfolgt.

6.3 Realisierung eines Vermittlungsplatzes

Die Realisierung eines umfassenden Vermittlungsplatz-Dienstes für heterogene Umgebungen ist im Rahmen des Projektes nicht beabsichtigt. Für den Vermittlungsplatz-Dienst der Universität Hannover wurde jedoch prototypisch eine WWW-basierte Lösung zur Abfrage der Callmanager entwickelt, um die Suche nach IP-Telefonnummern und Teilnehmern am Vermittlungsplatz der Telefonzentrale zu ermöglichen. Das System stellt in einem WWW-Browser eine Eingabemaske zur Suche nach den Teilnehmern mit IP-Telefonen bereit. Nach Eingabe einer Suchanfrage ruft ein Skript auf dem WWW-Server mehrere Callmanager über deren http-Schnittstelle nach entsprechenden Namen und zugehörige Rufnummern ab. Anschließend verarbeitet das Skript die Rückgabewerte und sendet die entsprechend aufbereiteten Ergebnisse an den WWW-Browser. Die eigentliche Vermittlung erfolgt durch manuelle Eingabe der angezeigten Telefonnummer in das Vermittlungssystem.

Die Verwendung eines WWW-basierten Systems ermöglicht neben der einfachen Implementierung die notwendige Beschränkung auf einen ausgewählten Nutzerkreis (authentifiziert durch Username/Password) oder auf bestimmte Domänen (z. B. uni-hannover.de). Darüber hinaus lassen sich die übertragenen Daten einfach per SSL verschlüsseln.



7 Mandantenfähigkeit

7.1 Allgemeine Struktur der Mandantenfähigkeit

Mandantenfähigkeit eines Telefonie-Systems ist die Fähigkeit, auf einer gemeinsamen Hardwareplattform mehrere Einrichtungen (Mandanten) virtuell getrennt zu versorgen. Dieses Paradigma wird in den TK-Systemen auch als Firmentrennung bezeichnet. Durch die Mandantenfähigkeit eines Systems ist es möglich, Investitions- und Wartungskosten für die Betreiber wesentlich zu reduzieren. Es wird sichergestellt, dass jede virtuelle Einheit nur ihre eigene Umgebung wahrnimmt. Die Mandantenfähigkeit betrifft in erster Linie die Trennung der Rufnummernpläne, der Call Detail Records sowie in einigen Fällen auch die Trennung der Bündel zwischen der TK-Anlage und der OVSt. Einen wesentlichen Vorteil kann auch die Trennung der Management-Funktionalitäten für einzelne Mandanten bedeuten.

Für die IP-Telefonie erscheint eine dreistufige hierarchische Gliederung der Managementaufgaben zweckmäßig:

1. In der höchsten Hierarchie-Stufe erhält der Betreiber des IP-Telefonie-Systems die vollen Rechte über das System inklusive der Rechtevergabe an andere Teilnehmer.
2. In der mittleren Hierarchie-Stufe bekommen die lokalen Administratoren für einzelne Mandanten abgestufte Administrationsrechte. Sie dürfen z. B. den eigenen Rufnummernplan verwalten, neue Teilnehmer hinzufügen und ändern sowie Berechtigungen verwalten.
3. Auf der tiefsten Hierarchie-Stufe stehen die Teilnehmer. Diese dürfen Funktionen hinsichtlich eigener Endgeräte aktivieren bzw. deaktivieren.

Für die Durchsetzung organisationsweiter Policies ist es wichtig, dass die Administratoren einzelner Mandanten entsprechende Berechtigungen für die zentrale Aktivierung bzw. Deaktivierung einzelner Features bekommen.

Untersuchungen zur Mandantenfähigkeit sind nicht Teil des Pilotprojektes. Es wird lediglich ein Punktekatalog zu berücksichtigender Massnahmen für die Mandantenfähigkeit einer Lösung erstellt.

7.2 Massnahmen zur Mandantenfähigkeit

7.2.1 Service Provider

Berechtigungen

- Konfiguration des gesamten Systems, Änderung aller am Call Manager verfügbaren Service Parameter
- Überschreiben der von den Site Administratoren bzw. Usern gesetzten Einstellungen
- Einsicht in die Call Detail Records aller User

Technische Möglichkeiten

- Einrichtung überlappender Rufnummernpläne für mehrere Mandanten



- Einrichtung bzw. Einbindung eines zentralen Directory Services
- Konfiguration des Routings für das gesamte System bzw. für einzelne Mandanten unabhängig voneinander
- Rufnummernmanipulation getrennt nach Mandanten, sowohl an der Quell- als auch an der Zielrufnummer
- Bulk Administration (gleichzeitiges Einrichten oder Ändern von mehreren hundert bis tausend Accounts)
- Anwendung von Default-Konfigurationen auf einzelne Teilnehmer bzw. auf Gruppen von Teilnehmern/Mandanten

7.2.2 Mandanten Administrator

Berechtigungen

- Verwaltung des eigenen Rufnummernplans
- Konfiguration von Least Cost Routing – es muss hierbei aber die Möglichkeit bestehen, seitens des zentralen Administrators das Least Cost Routing für die Administratoren der Mandanten zu unterbinden
- Einrichtung von neuen Telefonnummern/Usern und die Deaktivierung existierender Teilnehmer
- Aktivierung/Deaktivierung von Rufnummernunterdrückung, Rufumleitung etc.
- Einrichtung der Extension Mobility für bestimmte User und Endgeräte
- Services Freischalten und Sperren
- Zusätzliche Services einrichten und den eigenen Nutzern unabhängig von anderen Mandanten anbieten

Technische Möglichkeiten

- Verwaltung und Integration von Unternehmensverzeichnissen
- Einrichtung firmeninterner Outlook Integration

7.2.3 User

Berechtigungen

- Aktivierung/Deaktivierung der Rufnummernunterdrückung
- Einrichtung der Rufumleitung – permanent, bei besetzt, nach Zeit
- Auswahl der Klingeltöne (evtl. soll das vom Site-Administrator unterbunden werden)

Technische Möglichkeiten

- Einsicht in die eigenen Call Details
- Pflege eines eigenen Adressbuchs
- Import von üblichen Adressbüchern (Outlook, LDAP)



8 Verfügbarkeitsaspekte

Die Gewährleistung einer hohen Verfügbarkeit stellt eine besondere Herausforderung an die IP-Telefonie dar. So sind die Nutzer der herkömmlichen Telefonie einen nahezu störungsfreien Betrieb gewohnt. Diese Zuverlässigkeit wird durch den verbindungsorientierten Betrieb der herkömmlichen Telefonie sowie SDH-Netze und TK-Anlagen erreicht, die maßgeblich für eine hohe Verfügbarkeit konzipiert wurden. Die Komponenten IP-basierter Netze sind dem gegenüber für einen verbindungslosen Betrieb ausgelegt, der vom Prinzip her gegen Überlast und Kompromittierung (z. B. durch Denial-of-Service Angriffe) anfälliger ist.

Der in diesem Projekt untersuchte Ansatz räumlich und z. T. administrativ getrennter Netze für IP-Telefone (VoIP-VLAN der T-Systems) und Callmanager (Service Area) sorgt für zusätzliche Aspekte bei der Diskussion der Verfügbarkeit. Die Verbindung dieser Netze über das G-WiN kann insofern als hochverfügbar angesehen werden, da die Netztopologie des G-WiN-Kernnetzes redundant ausgelegt ist und da hier ein entsprechendes Management durch den DFN-Verein (auf IP-Ebene durch das DFN-NOC) bzw. die T-Systems (untere Netzebenen) gegeben ist. Die nachfolgende Diskussion beschränkt sich daher auf die Verfügbarkeit in den LANs für die IP-Telefone und die Service Area. Darüber hinaus werden grundlegende Aspekte der Verfügbarkeit des Datennetzes, wie z. B. das Monitoring von Komponenten einschließlich entsprechender Alarmierung von Mitarbeitern, nicht weiter erörtert.

8.1 Verfügbarkeitsaspekte im LAN

Dem Unternehmensnetzwerk (LAN) fällt als Transportmedium für die Signalisierungs- und Sprachdaten bei Einsatz von VoIP eine zentrale Rolle zu. Vor der Einführung von VoIP muss deshalb geprüft werden, ob das LAN in der Lage ist, die Echtzeit-Anforderungen von VoIP hinreichend gut zu erfüllen. Zu diesen Anforderungen gehört neben einer hohen Verfügbarkeit auch eine ausreichende Dienstqualität (QoS).

8.1.1 Layer-2 Dienstqualität

Die Struktur des Netzes und seine Dimensionierung beeinflusst maßgeblich die Dienstqualität. Als minimaler Standard ist ein durchgängig mit Switches ausgestattetes Netzwerk zu fordern. Auf einem „Shared Medium“ wäre hingegen, bedingt durch Kollisionen und Zugriffsverzögerungen auf das Medium, keine annähernd zuverlässige Einhaltung von QoS-Parametern möglich.

Die notwendige Übertragungsqualität von VoIP-Paketen über ein geschwitchtes Netz kann mittels zweier verschiedener Ansätze realisiert werden. Der erste sieht eine Überdimensionierung des Netzes (Overprovisioning) vor. Bei diesem Ansatz wird eine deutlich höhere Übertragungskapazität zur Verfügung gestellt als in der Hauptverkehrszeit abgerufen wird. Vorteil dieses Verfahrens ist die einfache Implementierung, da lediglich Netzkomponenten höherer Leistung einzusetzen sind. Ein zusätzlicher Aufwand für das Management entsteht nicht.



Der zweite Ansatz sieht eine Priorisierung der Daten und somit eine gezielte Ungleichbehandlung der Ethernet-Rahmen durch die Switches vor. Mit dieser Methode kann ein Kapazitätsmanagement betrieben und auch auf knapp dimensionierten Strecken eine hinreichende Dienstqualität erreicht werden. Der Einsatz dieser Verfahren geht jedoch mit einem nicht unerheblichen Aufwand zur Konfiguration und Überwachung einher und erfordert entsprechend höhere personelle Ressourcen.

Für den Anschlussbereich sollten Ethernet-Switches mit mindestens 100 MBit/s Transfer-rate dimensioniert werden. Ein Kapazitätsmanagement durch Priorisierung von Ethernet-Rahmen sollte auf knapp dimensionierte Strecken beschränkt bleiben.

8.1.2 Layer-2 Verfügbarkeit

Die zweite Anforderung bei der Einführung von VoIP an ein LAN ist dessen Verfügbarkeit. Diese hängt unter anderem von der Sicherung der Stromversorgung der Komponenten ab. Weitere Maßnahmen umfassen die Absicherung gegen Hardwareausfälle. Eine Möglichkeit zur Absicherung gegenüber begrenzten Ausfällen besteht darin, mehrere Interfaces auf einem Switch zu einem so genannten Channel zusammenzufassen und damit mehrere Switches zu koppeln. Channeling fängt somit Ausfälle einzelner Interfaces oder Kabel ab, schützt jedoch nicht bei Ausfall eines kompletten Switches.

Um den vollständigen Ausfall von Komponenten komplett überbrücken zu können, müssten diese redundant ausgelegt werden. Diese Maßnahme ist jedoch kostenintensiv und wird daher, mit Ausnahme des lokalen Backbones, selten ergriffen. Eine Alternative zu komplett redundant ausgelegten Backbones bietet sich in dem Aufbau einer Ringstruktur im lokalen Backbone mit der redundanten Anbindung der Switches über alternative Pfade. Die Verbesserung der Verfügbarkeit ist zwar gegenüber einem voll redundant ausgebauten Backbone geringer, die ringförmige Struktur ist jedoch bedeutend kostengünstiger. Für diesen Ansatz sollten zudem Protokolle wie das Rapid Spanning Tree Protocol (RSTP), die eine kurze Umschaltzeit nach einem Ausfall bieten, verwendet werden.

Zur Sicherstellung der Layer-2 Verfügbarkeit muss eine Versorgung der Netzkomponenten mit einer unterbrechungsfreien Stromversorgung (USV-Versorgung) vorausgesetzt werden. Der Anschlussbereich sollte zudem so dimensioniert werden, dass die IP-Telefone über Inline-Power (Power over Ethernet) versorgt werden können. Der Backbone sollte möglichst redundant ausgelegt werden, für den Anschlussbereich sollten Ersatzgeräte vorgehalten werden.

8.1.3 IP-Telefone

Die IP-Telefone stellen im Netzwerk keinen Single Point of Failure dar, da der Ausfall eines Gerätes lediglich dessen Nutzer betrifft. Zur Erhöhung der Verfügbarkeit, sollte die Stromversorgung der Telefone über Inline-Power erfolgen. Hierbei speist der Switch die angeschlossenen IP-Telefone über die Datenleitung mit Strom. Sind die Switches über eine USV abgesichert, ist eine Notversorgung der Telefone weitgehend garantiert. Um





Störungen durch den Ausfall der Versorgung mit Inline-Power abzusichern, können für die IP-Telefone zusätzlich Netzteile vorgehalten werden.

Die Sicherung der Stromversorgung der IP-Telefone durch Inline-Power ist sehr zu empfehlen. Der Einsatz von Netzteilen an Telefonen mit höherer Priorität, wie z. B. in öffentlichen Bereichen, ist als zusätzliche Sicherungsmaßnahme ebenfalls ratsam. Weiterhin sollte eine Anzahl IP-Telefone und Netzteile als Ersatz vorgehalten werden.

8.2 Verfügbarkeitsaspekte in der Service Area

8.2.1 Callmanager

Der Callmanager stellt die zentrale Komponente des VoIP-Systems dar. In der im Projekt aufgebauten Testkonfiguration befindet er sich in einer Service Area des Dienstleisters, die über ein WAN erreichbar ist. Da bei einem Ausfall des Callmanagers keine neuen Gespräche vermittelt werden können und somit der Betrieb nicht aufrechterhalten werden kann, ist eine redundante Auslegung zwingend erforderlich. Der redundante Callmanager ist im idealen Fall an einem anderen Ort als der primäre Callmanager installiert und zudem über eine andere Verbindung – oder sogar ein alternatives Netz – angebunden. Darüber hinaus kann über SRST (s. Kap. 4.1) das VoIP-Gateway kurzzeitig die rudimentäre Funktionalität des Callmanagers übernehmen.

8.3 Firewall

Für die PIX Firewalls in der Service Area gilt entsprechendes wie für die aktiven Netzkomponenten oder den Callmanager. In jedem Fall müssen die Firewalls redundant ausgelegt werden, es sollten sogar Ersatzgeräte vorgehalten werden.

8.4 Update-Management

Cisco Callmanager sowie PIX Firewalls arbeiten mit Software, die regelmäßig durch Updates und Patches aktualisiert wird. Letztere dienen hauptsächlich der Fehlerbeseitigung und müssen aus Sicherheitsgründen häufig sehr zeitnah eingespielt werden. Auf die Planung von Updates, die lediglich neue Funktionalitäten bieten, kann in der Regel mehr Zeit verwendet werden. Beiden Vorgängen ist gemeinsam, dass der Regelbetrieb für mindestens die Dauer des Neustarts der Systeme unterbrochen ist.

Durch den Einsatz redundanter Systeme, wie z. B. einem zweiten VoIP-Gateway oder Callmanager, können Unterbrechungen häufig stark verkürzt werden. Eine Vermeidung von Ausfällen ist aber nur selten möglich. Die Intervalle, in denen solche Arbeiten durchgeführt werden, müssen somit sehr sorgfältig geplant und in die Zeiten mit geringem Verkehrsaufkommen gelegt werden. Auch sollten die Benutzer rechtzeitig auf geeignetem Wege über die zu erwartenden Störungen informiert werden.





9 Security

Bereits von herkömmlichen TK-Anlagen sind Szenarien für Gebührenbetrug oder das unbefugte Abhören von Gesprächen bekannt. Dieser Missbrauch wird ermöglicht, indem zum einen der Betrieb unter fahrlässigen Sicherheitsstandards (häufig z. B. durch Nutzung von Default-PINs) durchgeführt wird, zum anderen indem erweiterte Leistungsmerkmale genutzt oder Signalisierungen gefälscht werden [Fer97].

Entsprechende Szenarien lassen sich ohne Einschränkung auch auf die Betrachtung Security-relevanter Aspekte der IP-Telefonie übertragen, wobei ausdrücklich die Abwehr von Denial-of-Service Angriffen einbezogen werden muss. Ähnlich zu den Betrachtungen der Verfügbarkeit kann hierbei zunächst die Verbindung zwischen dem VoIP-VLAN der T-Systems in der Einrichtung und der Service Area des Dienstleisters ausgenommen werden. Eine Authentifizierung und Verschlüsselung der Daten über ein z. B. IPsec-basiertes VPN zwischen VoIP-Gateways oder einer vorgelagerten Firewall sowie der Service Area schafft hier weitgehende Sicherheit.

Bei der Konzeption der LANs sind hingegen verschiedene Aspekte der Security zu beachten, die sich in vier Bereiche gliedern lassen:

1. VoIP-VLAN,
2. IP-Telefone,
3. VoIP-Gateways,
4. Übergang vom VoIP-VLAN zum G-WiN, über das der Callmanager in der Service Area zu erreichen ist.

Um im Folgenden auch die aktuelle Entwicklung von Security in VoIP geeignet zu berücksichtigen, werden neben den im Projekt gewonnen Erkenntnissen auch Angaben aus [Hal04] übernommen.

9.1 VoIP-VLAN

Die IP-Telefone sind in einem VoIP-VLAN zusammengefasst, dem keine anderen Geräte zugeordnet werden. Diese Zuordnung ist jedoch nicht abgesichert. Angreifer können sich ohne spezielles Know-how in das VoIP-VLAN einbuchten, wenn sie physischen Zugriff auf eine Netzwerkdose haben, auf die dieses VLAN geschaltet ist. Mit einem unmittelbaren Zugang zum VoIP-VLAN sind Denial-of-Service Angriffe oder DHCP-Angriffe möglich. DHCP-Angriffe können z. B. so ablaufen, dass sich ein Angreifer bis zur Erschöpfung des IP-Adresspools im DHCP-Server Adressen zuweisen lässt. IP-Telefone, deren DHCP-Lease abgelaufen ist, können nachfolgend keine neue IP-Adresse zugeteilt bekommen und sind für den Benutzer nicht mehr verfügbar.

Um Angriffe dieser Art zu erschweren, muss das VoIP-VLAN gegen unbefugte Geräte abgesichert werden. Um dies zu erreichen, bieten sich mehrere Mechanismen an:

1. Port-Security auf Cisco-Switches: Dieser Mechanismus bietet die Möglichkeit, einem Switch-Port fest eine MAC-Adresse zuzuordnen. Damit wird es unmöglich, ein fremdes Gerät an einen Switch-Port anzuschließen. Nicht verhindert werden kann damit



allerdings das Spoofen, also das Fälschen von MAC-Adressen. Somit bietet diese Funktion lediglich einen wirksamen, aber nicht absoluten Schutz gegen Fremdgeräte im VoIP-VLAN.

2. IEEE 802.1x: Das Protokoll IEEE 802.1x bietet die Möglichkeit, Benutzer an einem Switch-Port zu authentisieren und erst nach erfolgreicher Anmeldung den Switch-Port freizuschalten. Auch dieses Verfahren verhindert den Einsatz von fremden Endgeräten im LAN nicht vollständig, erschwert ihn aber durch den Einsatz sicherer Authentisierungsverfahren erheblich. IEEE 802.1x ist zum gegenwärtigen Zeitpunkt nicht in den Cisco IP-Telefonen implementiert.
3. VLAN Management Policy Server (VMPS, [Cis02]): Dieses Protokoll bietet eine dynamische Zuordnung von MAC-Adresse und VLANs. Endgeräte, deren MAC-Adressen im System bekannt sind, können an verschiedenen Switch-Ports ohne Änderungen der Konfiguration betrieben werden. Auch hier ist kein Schutz vor MAC-Spoofing gegeben.

9.2 IP-Telefone

Die IP-Telefone bilden das Frontend des Systems für die Nutzer. Angriffe auf ein IP-Telefon wirken sich in der Regel auf die Nutzung dieses Telefons aus. Auswirkungen können z. B. ein Denial-of-Service, Gebührenbetrug oder das Mithören von Gesprächen über Man-in-the-Middle Angriffe sein. Um Man-in-the-Middle Angriffe zu erschweren wird empfohlen, die Annahme so genannter Gratuitous-ARP Pakete auf den IP-Telefonen abzuschalten. Dies ist mit dem Cisco Callmanager ab Version 3.3(3) möglich.

Cisco IP-Telefone verfügen über einen integrierten 3-Port Switch. Ein Port an diesem Switch dient zum Anschluss eines weiteren Endgerätes, z. B. des Arbeitsplatz-PCs des Benutzers. Als Default-Einstellung ist das VoIP-VLAN auch auf diesem Port verfügbar. Somit kann jedoch an den Port auch ein weiteres IP-Telefon angeschlossen werden. Um das Mithören, sowie Angriffe über diesen Port zu erschweren, wird empfohlen, das VoIP-VLAN auf diesem Port der Telefone abzuschalten.

Auch der Einsatz von signierten Phone-Loads auf den IP-Telefonen ist zu empfehlen. Nachdem auf einem IP-Telefon zum ersten Mal eine signierte Phone-Load verwendet wurde, wird das Überspielen mit einer nicht von Cisco signierten Phone-Load abgelehnt. Diese Maßnahme verhindert die Manipulation der Phone-Loads z. B. über einen fremden TFTP-Server.

Sinnvoll ist auch das Feature „Extension Mobility“. Mit dieser Funktionalität muss sich der Nutzer gegenüber dem System am IP-Telefon authentisieren. Weiterhin können Zeiten konfiguriert werden, zu denen alle Benutzer automatisch abgemeldet werden, z. B. während der Nachtstunden. Im abgemeldeten Zustand können die Telefone als nicht amtsberechtig geschaltet werden, so dass ein Gebührenbetrug erschwert wird.

Ab Callmanager Version 4.0 lässt sich der HTTP-Server auf den IP-Telefonen, über den Status- und Konfigurationsinformationen abgerufen werden, abschalten. Diese Maßnahme ist zu empfehlen, da die abgerufenen Informationen zu Angriffen genutzt werden könnten. Weiterhin ist vorstellbar, dass mit einem Buffer-Overflow Angriff auf den HTTP-Server die Kontrolle über das IP-Telefon erlangt werden könnte.



Ebenfalls ab Callmanager 4.0 ist ein Mechanismus zur Authentisierung von IP-Telefonen gegenüber dem Callmanager und umgekehrt implementiert. Ebenso lässt sich eine Authentisierung der IP-Telefone untereinander während des Gesprächsaufbaus verwenden. Diese Funktionalität ist auf Cisco IP-Telefonen der Serien 7940/7960 verfügbar. Auf den neueren Geräten des Typs 7970 kann zusätzlich der Gesprächskanal über das Secure Realtime Protocol (SRTP) [BMN+04] verschlüsselt werden. Die Verwendung dieser Mechanismen sollte bei Verfügbarkeit entsprechender Endgeräte und Softwareversionen im Einzelfall überprüft werden.

9.3 VoIP-Gateways

Die VoIP-Gateways stellen die Schnittstelle zwischen VoIP-VLAN und OVSt dar. Sie sind damit in heterogenen Umgebungen installiert und sowohl aus IP-Netzen als auch aus dem herkömmlichen Telefonnetz angreifbar. Bei den im Projekt verwendeten Gateways handelt es sich um Router der Serie Cisco 26xx. Diese Geräte können derzeit als relativ sicher angesehen werden, d. h. es existieren wenig bekannte Angriffsmechanismen. Es ist jedoch zu empfehlen, auf neuere IOS-Versionen mit Bug-Fixes zu achten sowie mittels Access-Listen den Zugriff auf diese Systeme zu beschränken.



9.4 Übergang zwischen G-WiN zum VoIP-VLAN



Die umfassende Administration von einem entfernten Standort wie der Service Area schließt den direkten Zugriff auf die VoIP-Gateways und auf die IP-Telefone im VoIP-VLAN ein. Da dieser Zugriff über das G-WiN erfolgt, ist eine entsprechende Absicherung vor unberechtigtem Zugang unumgänglich. Deshalb wird der Einsatz einer Firewall mit Application-Level Gateway für die verwendeten Protokolle zur IP-Telefonie empfohlen. Die Firewall sollte am Übergang zwischen Daten-VLAN der Einrichtung und dem VoIP-VLAN der T-Systems platziert werden.

9.5 Callmanager

Der Callmanager stellt in einer VoIP-Umgebung die zentrale Komponente dar. Aus diesem Grund muss er gesondert geschützt werden. Folgende Schutzmaßnahmen sind zu empfehlen:

1. Der Callmanager sollte generell durch eine Firewall mit Application-Level Gateway geschützt werden. Diese Forderung ist typisch durch eine Cisco PIX Firewall gegeben.
2. Es ist täglich zu überprüfen, ob neue Updates für das verwendete Betriebssystem MS Windows 2000 vorliegen. Gegebenenfalls sind die Updates zeitnah während eines Wartungsfensters zu installieren.
3. Der Cisco Security Agent (CSA) sollte eingesetzt werden, um noch nicht erkannte Softwarefehler abzufangen.



10 Zusammenfassung

Mit diesem Beitrag werden zahlreiche Aspekte dargestellt, die bei der zentralen Bereitstellung eines VoIP-Dienstes sowohl vom Dienstleister als auch bei der Inanspruchnahme durch die jeweiligen Einrichtungen zu beachten sind. Die gesammelten Erkenntnisse wurden im Rahmen eines Projektes gewonnen, in dem ein solcher VoIP-Dienst über das G-WiN mit Komponenten der Firma Cisco von der T-Systems erbracht und an verschiedenen Einrichtungen der Universität Hannover sowie der TU Braunschweig unter der Projektleitung des RRZN erprobt wurde. Das Projekt zeigt, dass eine derartige zentrale Dienstleistung für einzelne Einrichtungen bereits heute möglich ist. Zahlreiche Aspekte wie Accounting und Billing, Verfügbarkeit, Security oder Mandantenfähigkeit bedürfen für einen DFN-weiten Einsatz jedoch weitergehender Betrachtungen, die ein breit gefächertes Know-how erfordern. Einrichtungen mit wenig Personal, bei denen die Ablösung einer herkömmlichen TK-Anlage ansteht, wird in jedem Fall empfohlen, die Bereitstellung der IP-Telefonie durch einen externen Dienstleister detailliert zu prüfen.

Der vorliegende Beitrag stellt lediglich einen Zwischenbericht aus dem laufenden Projekt dar. Der ausführliche Abschlussbericht ist nach dem Ende des Projekts im Sommer 2004 über den DFN-Verein oder direkt bei den Autoren verfügbar.

Literatur

- [BMN+04] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. *The Secure Real-time Transport Protocol (SRTP)*. IETF, RFC 3711, März 2004
- [Cis02] *Assigning Host-Based VLANs in Cisco Switch Products Using Cisco Secure User Registration Tool*. Cisco White Paper, 2002 http://www.cisco.com/warp/public/cc/pd/wr2k/urto/prodlit/urt_wp.pdf
- [FaMe04] P. Faltstroem, M. Mealling. *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*. IETF, RFC 3761, April 2004
- [Fer97] O. Ferreau. *Sicherheit im ISDN*. Technische Universität Darmstadt, Fachbereich Informatik, Diplomarbeit, Oktober 1997
- [GVE00] A. Gulbrandsen, P. Vixie, L. Esibov. *A DNS RR for specifying the location of services (DNS SRV)*. IETF, RFC 2782, Februar 2000
- [Hal04] J. Halpern. *SAFE: IP Telephony Security in Depth*. Cisco SAFE White Papers, <http://www.cisco.com/go/safe/>, Mai 2004
- [HoMo02] J. Hodges, R. Morgan. *Lightweight Directory Access Protocol (v3): Technical Specification*. IETF, RFC 3377, September 2002
- [HOO+03] S. Heinze, U. Oltmann, J. Ott, S. Prella, J. Rauschenbach, E. Scherer, E. Siemens. *IP-Telefonie im G-WiN*. DFN Mitteilungen, Heft 62, S. 6–9, Juni 2003
- [Mea02a] M. Mealling. *Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS*. IETF, RFC 3401, Oktober 2002
- [Mea02b] M. Mealling. *Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm*. IETF, RFC 3402, Oktober 2002
- [Mea02c] M. Mealling. *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database*. IETF, RFC 3403, Oktober 2002
- [Mea02d] M. Mealling. *Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application*. IETF, RFC 3404, Oktober 2002

