ComConsult Research

Der Netzwerk Insider

August 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

SIP Trunking und SIPconnect

bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

von Dipl.-Inform. Petra Borowka

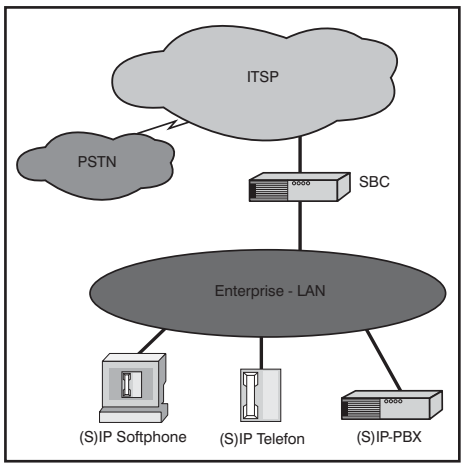
1. Die aktuelle Situation

Aktuell gibt es drei relevante Möglichkeiten, die Verbindung zwischen Enterprise-TK und öffentlich erreichbaren Teilnehmern zu fahren:

- Klassische PBX, hybride VoIP/ISDN Lösung
- proprietäres VoIP Trunking
- SIP Trunking

Klassische PBX und hybride VoIP / ISDN-Lösung

Aus der klassischen TK-Technik ist folgende Situation bekannt: zur Verbindung von zwei oder mehr TK-Anlagen wurden inter-



ne Trunks geschaltet und zur Verbindung einer Enterprise-Lösung mit dem weltweiten öffentlichen Telefonnetz wurden PSTN-Trunks geschaltet; beide Verbindungsarten wurden durch eine S_{2M}-Leitung oder Bündel von S_{2M}-Leitungen realisiert. Bei der Einführung von Voice over IP im Enterprise-Bereich werden mit so genannten hybriden Lösungen im Regelfall im ersten Migrationsschritt die vorhandenen S_{2M}-Leitungen auf PSTN-Gateways abgebildet, die Anzahl der angemieteten und monatlich bezahlten S_{2M}-Verbindungen bleibt gleich.

weiter auf Seite 21

Zweitthema

Sicherheit in Unified Communications

Integration und Sicherheit: Die Quadratur des Kreises?

von David Ferrest, Dr. Simon Hoff und Dr. Michael Wallbaum

Es gibt heutzutage kaum ein Unternehmen, in dem nicht UM-, CTI- oder Alarmserver ihren Dienst verrichten. In der alten TK-Welt konnten diese TK-Applikationen unter dem Aspekt der Sicherheit noch als vergleichsweise harmlos gelten. Die Schnittstellen zu den IT-Systemen waren - soweit überhaupt vorhanden - klar durch dedizierte Gateways definiert, die nur einen eingeschränkten Durchgriff auf die jeweils andere Seite ermöglichten. Die IT- und die TK-Welt bildeten somit funktionale Inseln, die nur durch wenige Brücken verbunden waren.

Im Kontext von Voice over IP (VoIP), d.h. mit einer gemeinsam durch IT- und TK-Komponenten genutzten Netzwerkinfrastruktur, stellt sich diese Situation jedoch drastisch anders dar. Per IP kann im Prinzip jede Komponente (Client oder Server) mit jeder anderen direkt kommunizieren.

Die Befürworter von VoIP und Unified Communications (UC) betrachten die bisherige Trennung von IT und TK durchaus zu recht als Produktivitätsbremse des Büroalltags.

weiter auf Seite 6

Neuer Kongress

Rechenzentrum Infrastruktur-Redesign Forum 2008

Seite 5

Geleit

Voice-over-IP-Forum 2008: der Markt am Wendepunkt?

ab Seite 2

Zum Geleit

Voice-over-IP-Forum 2008: der Markt am Wendepunkt?

Das ComConsult Voice-over-IP-Forum 2008 kommt zu einem kritischen Zeitpunkt. Der Markt ist an einem entscheidenden Wendepunkt angekommen:

- Traditionelle TK-Hersteller befinden sich im Umbruch und repositionieren sich bzw. werden das in den nächsten Monaten machen. Speziell Alcatel und Siemens sorgen hier zur Zeit für Aufmerksamkeit
- Provider stabilisieren ihre Service-Modelle für IP-Telefonie. SIP-Trunking öffnet sich als neuer Markt und bietet den Unternehmen neue Optionen (siehe Schwerpunktartikel)
- Wichtige neue Produkte wie Microsoft OCS sind jetzt fast ein Jahr auf dem Markt, das nächste Release steht an und damit bei vielen Anwendern der Übergang aus dem Testbetrieb in den Operativbetrieb
- Die Sicherheitslage hat sich stabilisiert und etabliert, auch wenn mit Unified Communications neue Risiken entstehen (siehe Zweitthema)
- Unified Communications kommt langsam aus dem Nebel. Der Leistungsumfang wird klarer, die Produktrealität ist besser bewertbar und eine seriöse Planung somit möglich
- Cisco, Microsoft, Polycom, Siemens und Tandberg haben die Diskussion über die Videokonferenz als elementarer Teil moderner Kommunikations-Lösungen neu belebt

Was bedeutet das nun? Im Kern geht es um die Frage, ob der Mehrwert der neuen Produkte inzwischen ein Niveau erreicht hat, dass die Installation traditioneller TK-Anlagen, auch wenn sie auf Hybrid-Niveau erfolgen würde, eine Fehlentscheidung ist (Hybrid bedeutet an dieser Stelle, dass die Anlage IP-Telefonie unterstützt, aber noch die traditionelle Anlagen-Architektur hat). Konkreter formuliert: ist die Zeit einer HiPath 4000, einer OmniPCX oder ähnlicher Produkte zu Ende? Oder positiv formuliert: bieten die neueren Architekturen einen solchen Mehrwert, dass sich ein weiterhin bestehendes Stabilitäts-Risiko lohnt?

Die Frage ist nicht neu, wir stellen sie seit 2 Jahren. Aber aus den zu Beginn genannten Gründen haben wir jetzt einen möglichen Wendepunkt erreicht.

Im Rahmen dieses Geleitworts dazu drei zentrale Anmerkungen:

1. Unified Communications

Heutzutage telefonieren wir nicht mehr, sondern wir kommunizieren unified. Jeder Hersteller sucht sich dabei aus dem möglichen Funktions-Spektrum das raus, was am besten zu seinen Produkten passt. Naturgemäß entstehen dadurch Defizite. Unsere Sichtweise dazu ist ganz klar: UC bedeutet für uns Orientierung an Geschäftsprozessen. Wichtige Prozesse sollen vereinfacht werden, Kommunikation soll schneller und effizienter werden. Alle Hersteller, die dies mit ihren Produkten gar nicht können, reduzieren dies typischerweise auf die Präsenz-Anzeige. Dabei muss klar gesagt werden, dass eine Reduzierung von Geschäftsprozessen auf eine Präsenzanzeige grober Unfug ist. Zum einen bezweifle ich ganz eindeutig, dass die Idee der schnelleren Erreichbarkeit wirklich messbar umgesetzt werden kann. Der Aufwand der Regel-Konfiguration lohnt sich nur für wenige Gesprächspartner. Damit fällt dieser ganze Bereich für beliebig viele Geschäftsprozesse (zum Beispiel mit Zulieferern und Kunden) weg. Zum anderen garantiert schnelle Erreichbarkeit keine erhöhte Effizienz. Diese kommt in der Regel aus sauber aufbereiteter und gut zugreifbarer Information. An dieser Stelle unterscheiden sich zum Beispiel interne und externe Geschäftsprozesse deutlich. Intern wird man zu 90% die Informations-Bereitstellung über eine Web-basierte Kollaborations-Plattform als kostengünstiger und effizienter bevorzugen. Zudem sind hier mögliche Erweiterungen einfacher und schneller umsetzbar. Extern wird aus heutiger Sicht SIP der Träger aller Effizienz-Verbesserungen sein. Weitergehende Informationen wie Bilder, Diagramme oder Videos müssen in das laufende Gespräch eingebunden werden können.

Klares Statement: Unified Communications erfordert ein übergeordnetes und vollkommen Produkt-neutrales Design. Wir reden nicht über technische Basteleien, sondern über eine präzise Orientierung an Geschäftsprozessen. Diese kann nicht als Trivialrezept mit den Zutaten Präsenz und Sharepoint erreicht werden. Die ganze Diskussion muss weg von der Technik.

2. Offenheit

Wer Geschäftsprozesse und Effizienzverbesserungen wirklich ernst nimmt, der kann das nur mit offenen Lösungen erreichen. Die wirklichen Zugewinne liegen in der Kommunikation mit externen Partnern. Dies kann nur funktionieren, wenn sich alle Seiten an offene Standards halten. Jeder nicht genormte Codec, jedes nicht wirklich offene Gateway ist hier ein Hindernis. Wer von Offenheit redet und Kollaboration predigt, aber proprietäre Sprach- oder Video-Codecs einsetzt, der sagt nicht die Wahrheit.

3. Netzwerk-Eignung

Cisco und Microsoft haben die Diskussion über Quality of Service und die Eignung bestehender Netzwerke neu belebt. Dabei ist aus dem wirklichen Leben kommend folgendes festzustellen:

a) ja, es gibt die Projekte, in denen bestehende Netzwerke sich als Voice-ungeeignet herausgestellt haben. Das Problem liegt hier häufig an dem Phänomen, dass die Netzwerke die Anforderungen zu 100% der Zeit einhalten müssen. Die 3% Überlastung von WAN-Verbindungen, die bisher nicht aufgefallen ist, kann jedes VoIP-Projekt zum Platzen bringen.

Zweitthema

Sicherheit in Unified Communications

Integration und Sicherheit: Die Quadratur des Kreises?

Fortsetzung von Seite 1

David Ferrest ist seit 2007 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der IT-Security. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Videokonferenz-Systeme befasst.

Dr. Simon Hoff ist technischer Direktor bei der ComConsult Beratung und Planung GmbH und unter anderem verantwortlich für den Bereich IT-Sicherheit. Dr. Hoff blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb in den Bereichen IT-Infrastrukturen, mobiler und drahtloser Kommunikationssysteme zurück.

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Betrachtet man allein die möglichen Verbesserungen der Arbeitsabläufe, die sich durch die Integration ergeben, so spricht in der Tat alles für eine zunehmende Verschmelzung der unterschiedlichen Systeme. Berücksichtigt man jedoch auch die Auswirkungen der Integration auf Vertraulichkeit, Integrität und Verfügbarkeit des Gesamtsystems, so kann die Beurteilung von UC nicht mehr ganz so eindeutig ausfallen.

Dieser Artikel beschreibt einige für UC wichtige TK-Applikationen und betrachtet insbesondere die durch sie entstehenden Gefährdungen der IT-Sicherheit und analysiert entsprechende Sicherheitsmaßnahmen. Grundlage ist die im Juli 2008 veröffentlichte Technische Leitlinie Sichere TK-Anlagen des Bundesamts für Sicherheit in der Informationstechnik (siehe [1]).

1. Bausteine von Unified Communications

Die Funktionen eines UC-Systems bzw. die Applikationen im Umfeld einer TK-Anlage sind äußerst vielfältig und reichen vom klassischen Sprachmailbox-System bis hin zur Steuerung von Gebäudetechnik über das Telefon. Solche Applikationen können sich der Vermittlungsfunktion einer TK-Anlage bedienen, die Anlage und Endgeräte steuern oder Informationen verwerten, die von der Anlage bzw. über die Anlage bereitgestellt werden. Abbildung 1 zeigt eine Auswahl weit verbreiteter Funktionen.

Auch wenn keine der dargestellten Funktionen wirklich neu ist, so erhalten sie doch mit der wachsenden Verbreitung von VoIP eine zunehmend größere Relevanz. Der Wegfall von kostspieligen proprietären Gateways und der Einsatz standardisierter Protokolle senkt die Kosten und erlaubt die Erschließung neuer Anwendungsfelder. Die Hersteller setzen verstärkt auf diesen Trend und bieten unter dem Stichwort Unified Communications Systeme an, die vielfältige Möglichkeiten zur Kommunikation bieten - aber auch zum potenziellen Missbrauch.

Im Folgenden werden die wichtigsten der in Abbildung 1 dargestellten und in der Praxis häufig vorzufindenden TK-Applikationen bzw. UC-Funktionen sowie die von Ihnen verwendeten Protokolle und Schnittstellen beschrieben.

1.1 Unified Messaging

Unified Messaging (UM) integriert verschiedene Nachrichtenformate in einem einheitlichen System. Die Anwender entnehmen ihre Nachrichten (z. B. E-Mail, Fax, SMS und Sprachnachrichten) einer einzigen Datenbank bzw. können über eine einzige Nutzerschnittstelle Nachrichten unterschiedlichen Formats versenden. Viele UM-Systeme bieten zudem die Möglichkeit, auf diesen konsolidierten Nachrichteneingang über verschiedene Kanäle wie z. B. über eine Web-Oberfläche oder per Telefon zugreifen zu können.

Es muss betont werden, dass keine allgemein akzeptierte Definition des funktionalen Umfangs von UM existiert. So vertreiben einige Hersteller reine Sprachnachrichtensysteme unter dem Begriff UM, während Produkte anderer Hersteller nur den Empfang von Fax-Nachrichten im E-Mail-Postfach der Benutzer unterstützen. Im Folgenden wird der Begriff UM entsprechend der einleitenden Beschreibung sehr weit gefasst, um alle sicherheitsrelevanten Aspekte dieser Klasse von TK-Applikationen zu erfassen.

UM-Produkte mit einem umfassenden Funktionsspektrum benötigen naturgemäß

Sicherheit in Unified Communications - Integration und Sicherheit: Die Quadratur des Kreises?

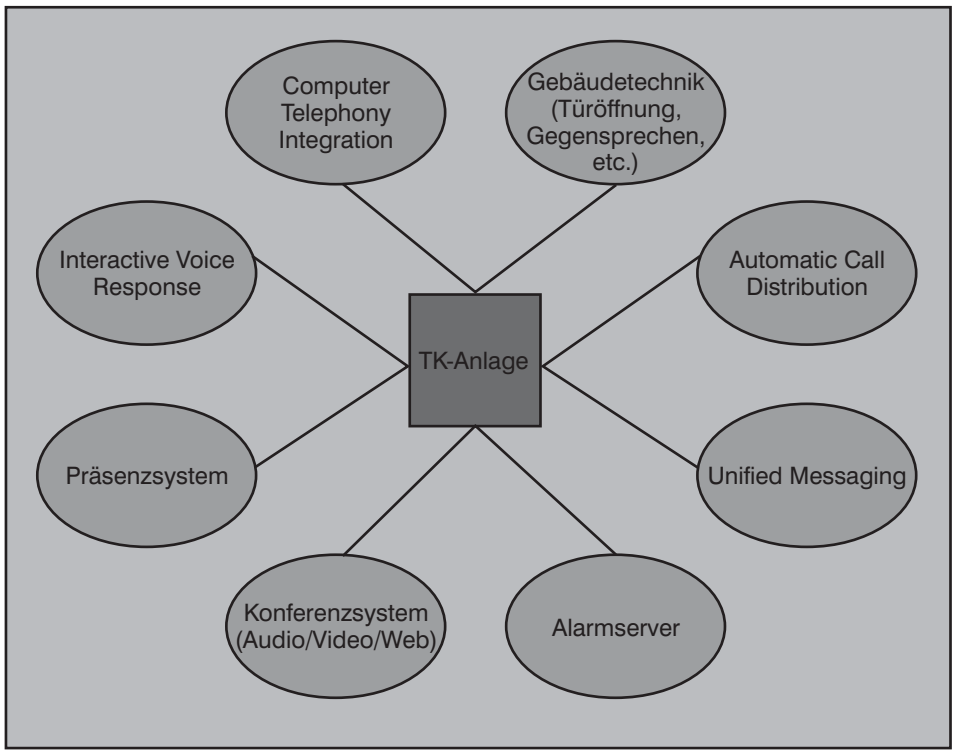


Abbildung 1: Applikationen und Mehrwertdienste mit Bezug zur Telekommunikation

eine Vielzahl von Schnittstellen für Benutzer sowie unterschiedliche Dienste und Anwendungen. Im Mittelpunkt stehen dabei die Schnittstellen zu TK-Anlagen und zu E-Mail-Systemen. Hinzu kommen noch Schnittstellen zur Kopplung mit anderen Kommunikationssystemen, Administrationsschnittstellen, Benutzerschnittstellen, Anbindungen an Verzeichnisdienste sowie Schnittstellen zu Geschäftsapplikationen (siehe Abbildung 2).

Für die Integration von UM-System und TK-Anlage werden (zumindest aus logischer Sicht) zwei Schnittstellen benötigt. Über eine Sprachschnittstelle werden von der TK-Anlage kommende Anrufe an das Sprachspeichersystem übergeben. Umgekehrt werden bei telefonischen Abfragen die Nachrichten über die Sprachschnittstelle ausgegeben. Die zweite Schnittstelle wird für Signalisierungsdaten benötigt, z. B. um Endgeräten zu signalisieren, dass neue Nachrichten auf den Benutzer warten, oder um die Ansage des Sprachspeichersystems an den jeweiligen Anrufer bzw. den Grund der Weiterleitung (besetzt, nicht verfügbar, etc.) anzupassen.

Die Integration mit klassischen TK-Anlagen und Hybrid-Systemen erfolgt in der Regel über eine in den UM-Server eingebaute Telefonie-Karte. Über diese Karte werden die Sprachdaten verarbeitet und bei einigen Produkten durch speziell kodierte Tonfolgen auch die Signalisierungsdaten.

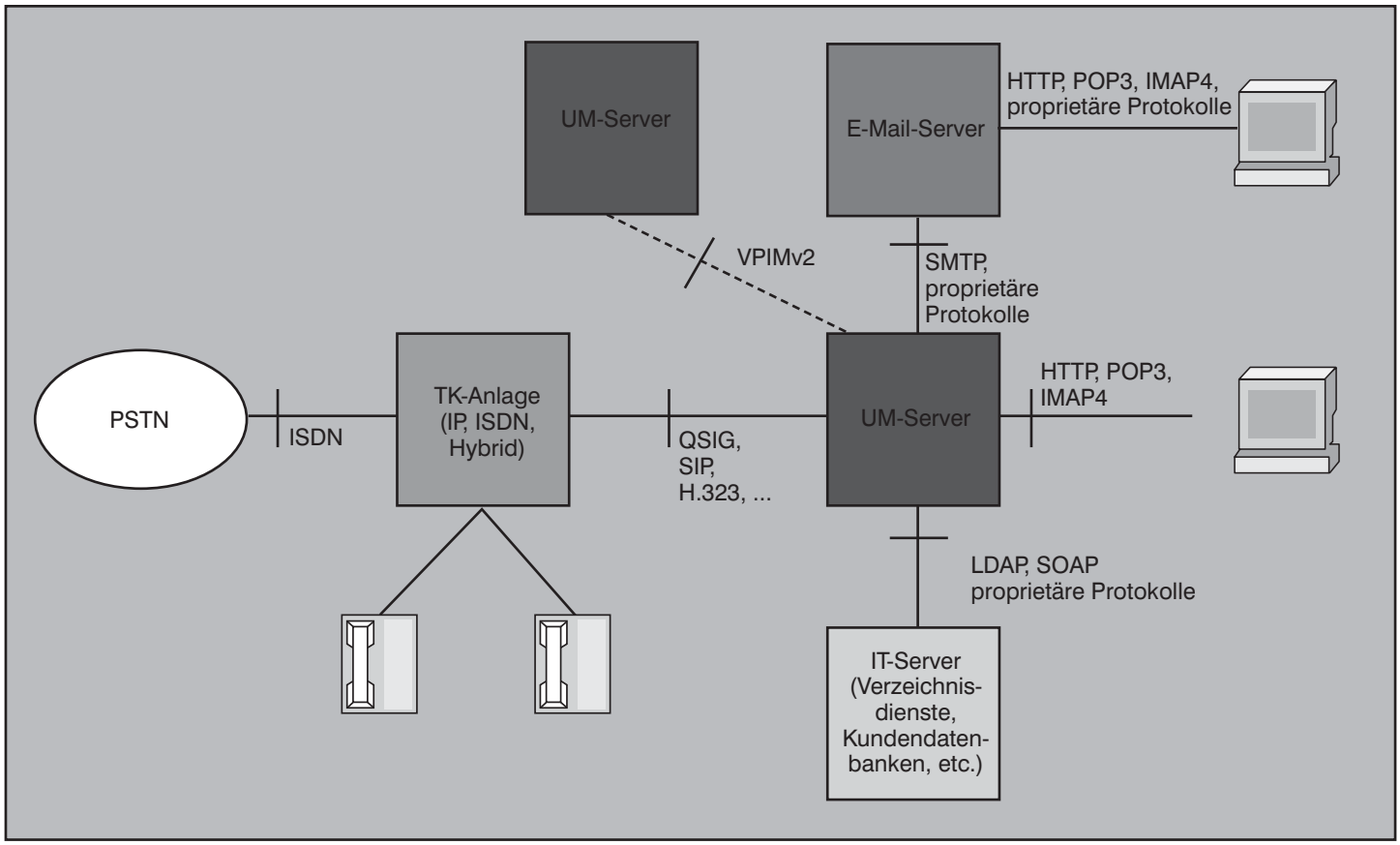


Abbildung 2: Typische Architektur eines Unified Messaging Systems mit Integration in ein IT-System

Schwerpunktthema

SIP Trunking und SIPconnect

bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

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.

Gespräche mit unternehmens-externen Teilnehmern werden weiterhin über zeittarifierte PSTN-Verbindungen gehandhabt (siehe Abbildung 1.1). Dies gilt insbesondere für Gespräche ins Ausland, die nach wie vor zu internationalen PSTN-Ferntarifen abgerechnet werden (siehe Abbildung 1.2).

VoIP Trunking

Sofern das Corporate IP-Netz über freie Bandbreite für TK verfügt oder aber entsprechend hochgerüstet wird, können interne und externe S_{2M}-Trunks ganz oder teilweise durch unternehmensinterne IP-Verbindungen abgelöst werden. Hier setzen viele LCR-Lösungen von VoIP Implementierungen an: Ein Gespräch wird über das Corporate IP Netzwerk bis an den Standort weitergeleitet, der am nächsten d.h. tarifgünstigsten zu dem angewählten PSTN Teilnehmer liegt. Über das dortige PSTN-Gateway wird das Gespräch ins PSTN-Netz weitergeleitet. Dadurch entstehen nur noch PSTN-Kosten für lokale Tarife, PSTN-Kosten für Ferntarife werden optimiert oder ganz vermieden, wie in Abbildung 1.3 gezeigt. Soweit die Kapazität des Corporate-IP Netzwerks überschritten ist, kann durch Call Routing und CAC-Regeln konfiguriert werden, dass die überzähligen Gespräche wie bisher direkt ab Ausgangsstandort über das PSTN geroutet werden.

Bei Ende-zu-Ende Nutzung einer einheitlichen Enterprise Lösung stehen mit dem Einsatz proprietärer IP-Trunks (Alcatel ABC, Avaya DCS, Nortel MCDN, Siemens CorNet etc.) zwischen den TK-Knoten viele bis alle Leistungsmerkmale standortübergreifend zur Verfügung. Werden unterschiedliche Hersteller eingesetzt, so bietet H.323 im Regelfall lediglich die Möglichkeit, Basic Call Funktionalität über IP Trunks zu nutzen, da die allermeisten Hersteller die Zusatzfunktionen (H.450) nicht unterstützen. QSIG mit einem etwas höhern Funktionsumfang von ca. 10 bis 20 Leistungsmerkmalen steht hier nicht zur Debatte, weil die meisten Hersteller QSIG nicht über IP unterstützen. Die-

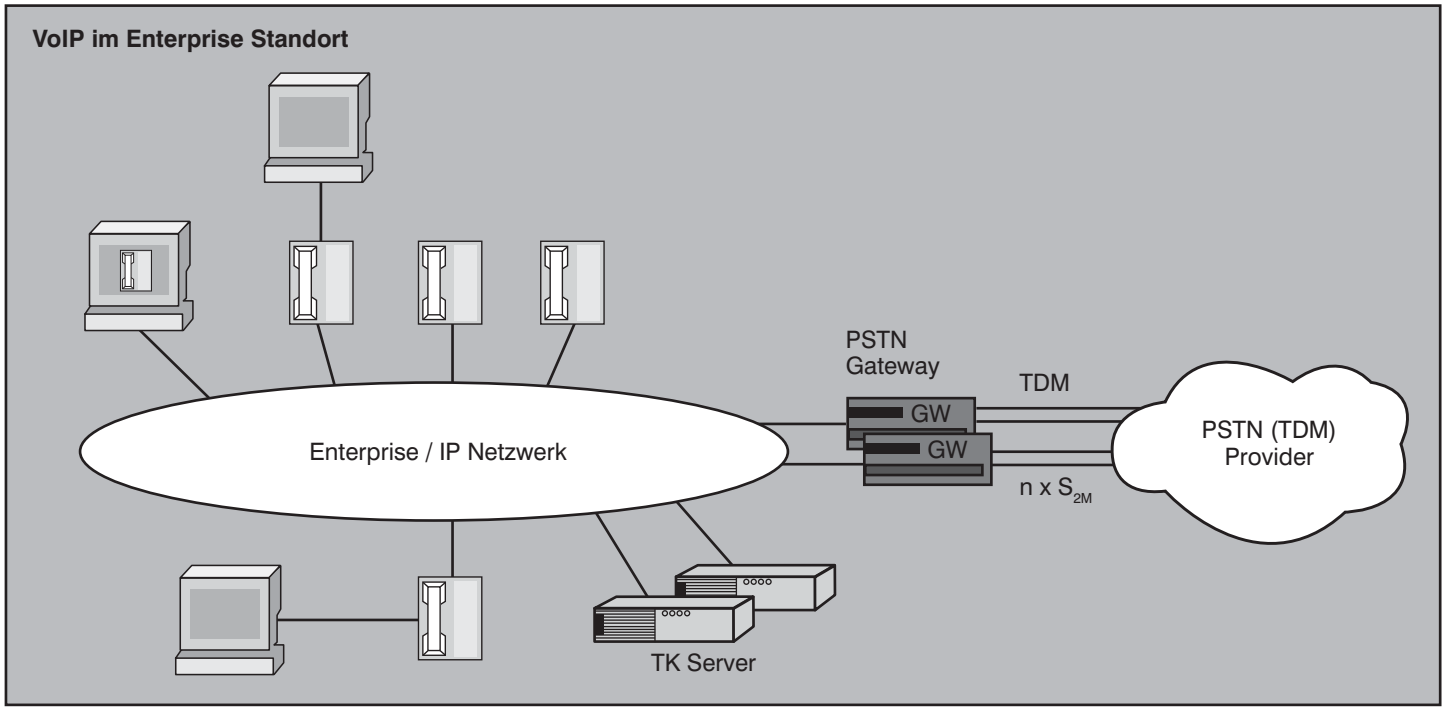


Abbildung 1.1: Hybride VoIP Lösung mit PSTN-Gateways

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

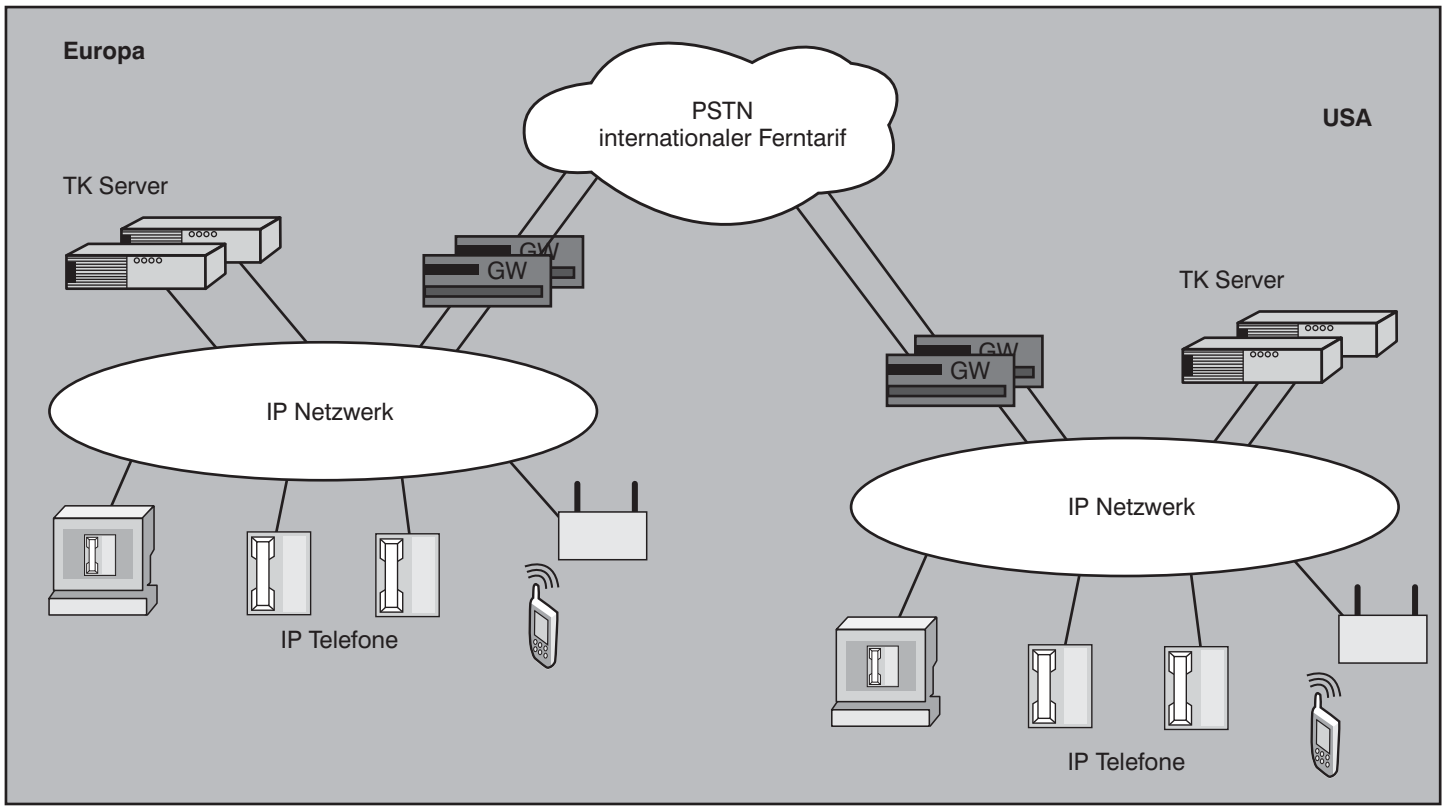


Abbildung 1.2: Hybride VoIP Lösung mit PSTN-Gateways je Standort

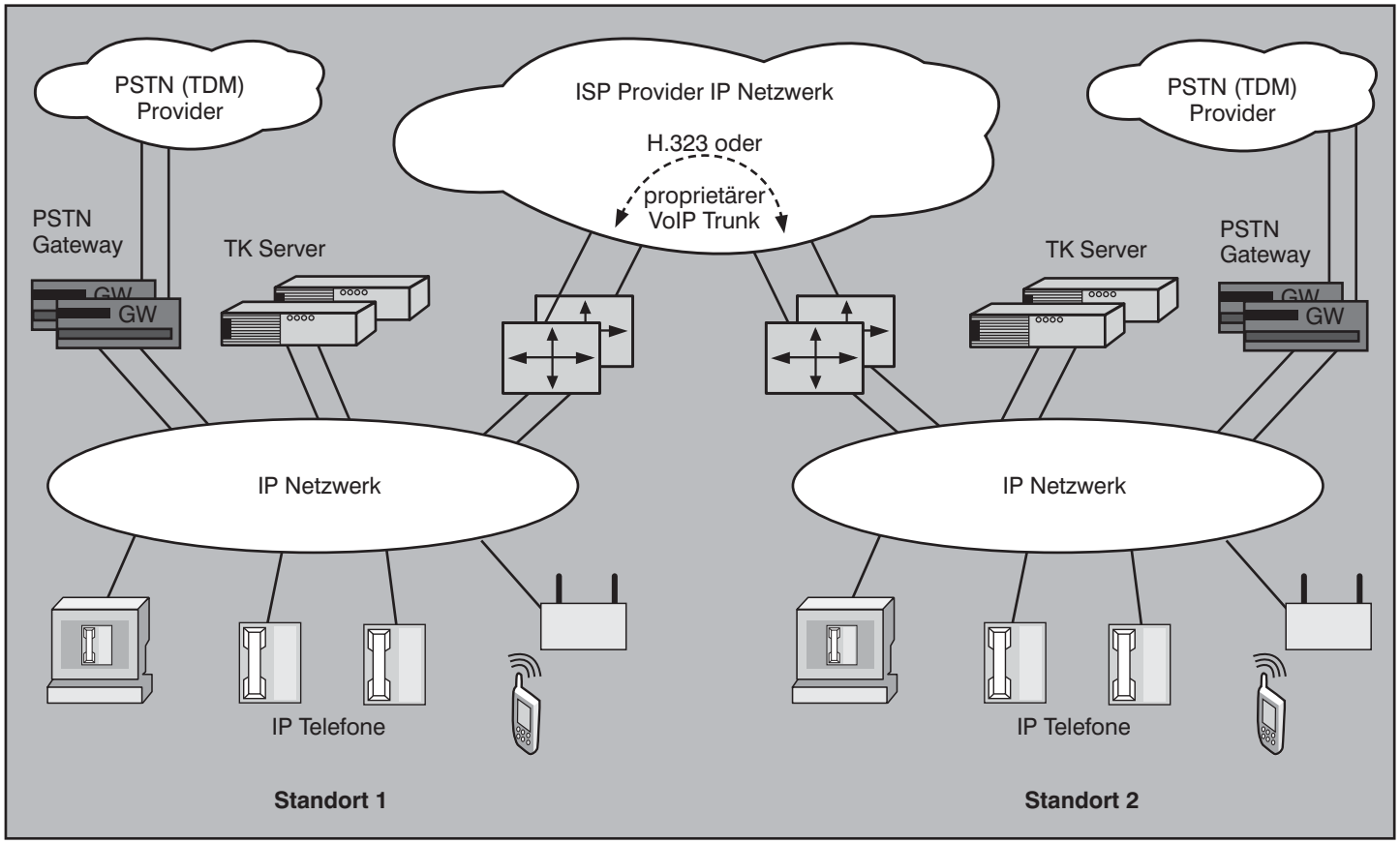


Abbildung 1.3: Nutzung des Corporate IP Netzwerks für Corporate VoIP Trunks