Dr. Suppan International Institute

Der Netzwerk Insider

Juni 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

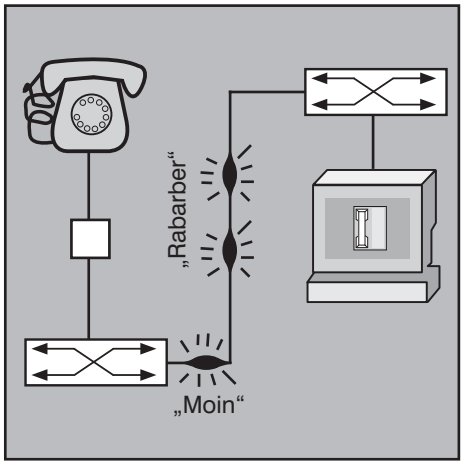
Design von „Voice-ready“ Netzen

von Dipl.-Inform. Petra Borowka

Der 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. Für eine Einführung in Voice Security und SIP verweisen wir auf die Netzwerk Insider März bis Mai 2004.

Im Rahmen dieses Beitrags werden wir auf folgende Betriebsziele und Optimierungs-Kriterien eingehen:

- Welche Verfügbarkeit braucht ein sprachgeeignetes Netzwerk?



- Welche Durchsatzanforderungen hat ein sprachgeeignetes Netzwerk?
- Wie effizient lässt sich die Netzwerkinfrastruktur nutzen?
- Kann Sprache flexibel als neuer Dienst integriert werden?
- Wie werden TK-Server eingebunden?
- Welche Antwortzeit fordert Telefonie?
- Ist Quality of Service erforderlich?
- Welche Skalierbarkeit wird mittelfristig benötigt?
- Welche Konsequenzen ergeben sich für Sicherheitsmaßnahmen?

weiter auf Seite 14

Zweitthema

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

(Fortsetzung - Mai 2004)

von Dipl.-Inform. Petra Borowka

Teil 2 beschreibt neue Anwendungen, die mit SIP zur reinen Telefonie hinzukommen: Instant Messaging, Anwesenheitsanzeige und Videokonferenz.

Auch Microsoft stellt seine Telefonie-Schnittstelle mit dem Windows Messenger von H.323 auf SIP um. Aber der Betrieb von SIP bereitet auch noch Probleme: Für Sicherheit und den Betrieb über Firewalls hinweg sind noch keine standardisierten Lösungen verfügbar. Abschließend geben wir ein Fazit zur Marktbedeutung und Produktreife von SIP.

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. Für eine Einführung in SIP verweisen wir auf den Netzwerk Insider vom Mai 2004.

weiter auf Seite 7

Top-Event

IP-Telefonie: Intensiv-Evaluierung und IP Betriebsgrundlagen

auf Seite 5

Zum Geleit

Neue Trends im Netzwerk- und System-Management

auf Seite 2

Report des Monats

Windows Server 2003 - Active Directory und IP-Management

auf Seite 12

Zum Geleit

Neue Trends im Netzwerk- und System-Management

In den letzten Monaten hat sich die Welt des Netzwerk- und System-Managements wieder einmal deutlich verändert. Zum einen sind Verschiebungen innerhalb der Funktions-Schwerpunkte zu beobachten, zum anderen gewinnen neue Themen immer mehr an Bedeutung.

Dabei sind alle Entwicklungen miteinander verzahnt, so dass Reduzierungen auf einzelne Änderungen häufig keinen Sinn machen. Im Endeffekt ist ein Redesign der vorhandenen Lösungen gefragt, das auch gleichzeitig zur Bereinigung der in den letzten Jahren angefallenen Administrations-Leichen dient.

Nachfolgend soll ohne Anspruch auf Vollständigkeit auf wichtige Entwicklungen eingegangen werden:

Schwerpunkt Netzwerk-Management

Netzwerke unterliegen weiter einem starken Wandel. Das aktuelle Schlagwort heißt Netzwerk-Konvergenz und beinhaltet die Integration neuer Anwendungsbereiche in Netzwerke, die bisher in eigenen, separaten Strukturen kommuniziert haben.

Mit dieser Konvergenz entstehen weiter gehende Anforderungen an eine geeignete Management-Lösung. Parallel verschiebt sich die Bedeutung von Netzwerk-Management. Netzwerk-Management ist auf dem besten Wege seine alte Bedeutung als zentrale und wichtigste Management-Technologie zurück zu erobern, allerdings unter völlig veränderten Rahmenbedingungen.

Zwei wichtige Themenbereiche der Konvergenz verdeutlichen als Beispiel sehr gut den Charakter der ablaufenden Änderungen im Netzwerk-Bereich.

Dies sind:
- die Integration von IP-Telefonie und
- die Eingliederung des Feldbus-Bereichs in der Fertigung.

Verallgemeinert kann festgestellt werden, dass sich mit Konvergenz nun Technologie-Bereiche im Netzwerk treffen, die völlig verschiedene Anforderungen an Netzwerke stellen.

Damit entsteht sofort der Bedarf nach einem Applikations- und Technologie-orientierten Netzwerk-Management, das den Bedarf einer Applikation gezielt abbildet.

Parallel erhöht sich innerhalb der nächsten 5 Jahre die Teilnehmerzahl in den Netzwerken durch diesen Trend massiv.

ComConsult Research prognostiziert eine Erhöhung, die im Einzelfall den Faktor 10 erreichen kann. Auch daraus entstehen weitergehende Anforderungen an das Client-Management. So wird die Trennung von Benutzern und Clients im Netzwerk und ggf. die Bildung von eigenen Überwachungsbereichen nur funktionieren, wenn die Clients identifiziert und zugeordnet werden können.

In den im Netzwerk laufenden Datenströmen wird dies häufig durch die Protokollzuordnung möglich sein, im Bereich der Zugangskontrolle wird aber eine Einzel-Identifikation unvermeidbar sein.

Die ablaufenden Veränderungen im Sinne der Zunahme der Teilnehmerzahlen generieren kein Lastproblem solange kabel-gebundene Netzwerke im Einsatz sind.

Hier steht der Wechsel auf 10 Gigabit im Rechenzentrum und im Backbone bevor. Speziell im Rechenzentrum wird er für zentrale Hochleistungskomponenten auch völlig unspektakulär erfolgen. Interpoliert man den Preisverfall und die Produktankündigungen der letzten Monate (speziell Cisco und Extreme), dann wird 10 Gigabit innerhalb von 3 Jahren Normalität werden.

Im Bereich der Funktionale nach IEEE 802.11 wird ein eigenes Management mit Technologie-spezifischen Überwachungs- und Alarmfunktionen entstehen müssen (Erkennung unzulässiger Access Points, Ausfall und Umschaltung von Access Points, Quality of Service-Management). Hierzu werden die Hersteller sicher in Kürze geeignete Module anbieten, die in die vorhandenen Management-Lösungen integriert werden können. Ggf. macht es auch Sinn, über eine messtechnische Lösung wie die von AirMagnet nachzudenken, die unabhängig von den Herstellern der eingesetzten WLAN-Komponenten eine Reihe der notwendigen Funktionen abdeckt.

Im Vordergrund aller notwendigen Veränderungen im Netzwerk stehen auf jeden Fall Strukturfragen. Im Mittelpunkt steht die Frage: ist unser bisheriges Netzwerk-Design tragfähig für die Integration völlig verschiedener Anwendungsbereiche mit einer starken Erhöhung der Teilnehmerzahlen oder bedarf es einzelner Änderungen.

Hier bleibt festzustellen, dass viele erfahrene Netzwerke diese Frage unterschätzen und mehr abwartend auf ihre starken Layer-3-Backbone-Netzwerke verweisen. Drei Beispiele sollen verdeutlichen, dass es damit nicht getan ist:

Beispiel 1

Mit der Integration von Feldbusbereichen auf der Basis von Ethernet müssen große Layer-2-Bereiche integriert werden. Die hier eingesetzten Geräte und Anwendungen sind häufig nicht Layer-3-tauglich. Gleichzeitig würden zum Teil aber so große Layer-2-Bereiche entstehen, dass dies das Risiko von Instabilitäten in sich birgt.

Beispiel 2

Das Thema Benutzertrennung im Netzwerk auch unter Berücksichtigung von mobilen Benutzern gewinnt stark an Bedeutung. Auf der Basis einer Einwahlprozedur sollen Endteilnehmern Rechte zugewiesen werden, von denen die Behandlung im Netzwerk abhängt. IEEE 802.1x kommt hier eine große Bedeutung zu. Ein gutes Beispiel für die Umsetzung derartiger Lösungen liefert Enterasys mit seinem UPN. Beachten Sie auch unser neues Seminar zu diesem Thema!

Neue Trends im Netzwerk- und System-Management

Beispiel 3

Aktuelle Sicherheits-Risiken haben zu einem Paradigmen-Wechsel im Bereich der Sicherheit geführt.

Jeder Betreiber sollte den erfolgreichen Angriff als unvermeidbar ansehen und sich mit der Frage der Handhabung befassen.

Das zentrale Thema ist die Sicherheits-Strukturierung von Netzwerken im Sinne der Bildung von Sicherheits-Zellen, die sich bei einem Angriff automatisch vom Rest des Netzwerks abkoppeln. Derartige Zell-Konstrukte können ein neues Backbone-Design erfordern, da sich solche Zellen über den gesamten Backbone erstrecken können und somit Teile des Backbones separiert werden können müssen (eine der Kernfragen ist genau, ob Sicherheits-Zellen auf abkoppelbare IP-Subnetze reduziert werden oder ob sich Zellen über Teile des Backbones erstrecken).

Mögliche Geräte sind hier ASIC-basierte Gigabit-Firewall mit IDS-Funktionalität wie sie zum Beispiel von Fortinet angeboten werden. Auch der Einsatz von MPLS im Campus-Backbone wird wieder ein Thema.

Es ist unschwer festzustellen, dass diese Entwicklungen Auswirkungen auf Netzwerk-Management haben. Zum einen muss die potenzielle Leistung von Netzwerken unter besonderer Berücksichtigung der konkreten Anforderungen einzelner Anwendungsbereiche überwacht werden. Zum anderen muss die Leistung, die Anwendungen real erfahren festgestellt werden.

Die Markt- und Produkt-Tendenzen sind dann auch klar:

Tendenz 1

Modellierung von Anwendungsbereichen analog zu den bisherigen Service-Modellen (Beispiel: ein Management-Abbild der Voice-Welt entsteht quasi als Service-Modell)

Tendenz 2

Erfassung der potenziellen Leistung von Netzwerken durch Verbindungs-Management auf der Basis von Applikations-spezifischer Kunstlast (Beispiel: die grundsätzliche Eignung der Netze für Voice oder für bestimmte Realzeittypen aus dem Produktionsbereich wird permanent überwacht, Packet-Loss-Raten, Jitter und Antwortzeiten werden gegenüber einem Normal dargestellt)

Tendenz 3

Erfassung der realen Netzwerk-Leistung ausgewählter Anwendungen (Beispiel: die reale Betriebssituation für eine Webapplikation wird überwacht, dies kann End-to-End oder auf Probe-Basis erfolgen)

Alle drei Trends finden sich in aktuellen Produkt-Ankündigungen wieder. Speziell im Bereich der Erfassung der realen Netzwerk-Leistung ausgewählter Anwendungen sind in den letzten Wochen seit der CeBIT mehrere Produkte angekündigt worden (siehe zum Beispiel die Netzwerk-Probe von Fluke).

Das traditionelle Netzwerk-Management wird damit nicht überflüssig. Die Überwachung der Basis-Verfügbarkeit der Netzwerk-Komponenten ist nach wie vor ein Muss. Aber alleine damit kann heute kein modernes Netzwerk mehr adäquat gemanagt werden.

Sicherheits-Management wird zum Schlüssel

Die Zahl eingesetzter Sicherheits-Komponenten nimmt permanent zu. Ein Beispiel ist die zunehmende Forderung nach Intrusion Detection als Mittel zur Erkennung erfolgreicher Würmer (siehe zum Beispiel Produkte von Toplayer). Mittlerweile sind der Reifegrad und die Erkennungs-Sicherheit in diesem Bereich gestiegen.

Ein weiteres Beispiel sind Applikations-orientierte Firewall-Lösungen, die zum Beispiel Angriffe auf http-Basis erkennen (siehe Nokia mit seinen neuen Zusatzlösungen zur Firewall 1, beachten Sie auch unser neues Seminar zur Umsetzung von Sicherheits-Lösungen von Web-Applikationen).

Mit der Zunahme der Komponentenmenge bei gleichzeitiger Ausweitung der Funktionalität der Sicherheits-Komponenten nimmt der Bedarf an Sicherheits-Operating weiter zu.

Eine wesentliche Teilkomponente ist dabei die automatische und zentralisierte Auswertung von Logfile-Einträgen. Dazu sind Produkte erforderlich, die fertige Filter für bekannte Logfile-Einträge anbieten. Leider beschränken sich diese Produkte auf sehr gängige Firewall- und Router-Systeme. Trotzdem zeigen Ansätze wie der von Intellitactics den generellen Trend in diesem Bereich auf.

Starke Überlappungen gibt es wie auch die genannten Beispiele zeigen zwischen der Umsetzung von System-Sicherheit und der Integration von Sicherheits-Lösungen in Netzwerke. In diesem Überlappungsbereich gewinnt das Thema Identity-Management eine immer höhere Brisanz.

Welche Benutzer existieren, welche Accounts sind zugeordnet, von welchen Ge-

räten, von welchen Orten dürfen sie auf welche Daten und Applikationen zugreifen. Gerade die zur Zeit beginnende Umsetzungswelle von IEEE 802.1x-Projekten trifft genau diesen Funktionsbereich. Auch die großen Hersteller von Management-Lösungen haben diesen Trend erkannt wie zum Beispiel die aktuellen Ankündigungen von Hewlett Packard zu diesem Thema zeigen.

Web-Management

Software-Architekturen sind in einem massiven Umbruch. Nahezu jedes größere Unternehmen arbeitet an der Bereitstellung von Web-Applikationen zum standort-übergreifenden Zugriff auf zentrale Daten und Geschäftsprozesse.

Auch Kollaborations-Lösungen nehmen im Zeitalter der Globalisierung immer mehr zu (siehe Ankündigungen von Alcatel, Cisco, Siemens zum Thema Dokumenten-Sharing, White-Board, Video auf Basis von SIP).

Dabei ist festzustellen, dass viele Unternehmen gerade im Management von Web-Anwendungen schwere Defizite haben. Von der generellen Verfügbarkeit bis hin zur Antwortzeit von Einzeltransaktionen reichen die Management-Funktionen, die erbracht werden müssen. Da sinnvolle Analysen den Einsatz von Remote-Agenten erfordern, die die Sichtweise der Anwender/Kunden repräsentieren ist hiermit auch der gesamte Themenbereich Rollout und Steuerung von Agenten betroffen.

Auf jeden Fall muss der gesamte Bereich der Webapplikationen eine eigene Management-Repräsentanz erhalten, da Störungen in diesem Bereich wichtige nationale und internationale Abläufe behindern können. Die Vision, dass Mitarbeiter an allen Orten der Welt in alle gewünschten Geschäftsprozesse komplett integriert werden können erfordert eine begleitende Management-Lösung.

Fazit

Dies waren nur ausgewählte Beispiele ohne Anspruch auf Vollständigkeit. Sie zeigen, dass Netzwerk- und System-Management erneut in Bewegung geraten ist. Vorhandene Lösungen müssen erweitert, zum Teil völlig neue Funktionsbereiche aufgebaut werden.

Der Druck ist hoch, entsprechend hoch ist auch die Zahl der Produkte und Technologien, die neu in den Markt drängen. Doch nicht alle diese Produkte haben eine Zukunft. Zum Teil erfüllen sie nicht, was sie versprechen, zum Teil repräsentieren sie reine Mode-Erscheinungen ohne langfristige Perspektive.

Hier setzt unsere Hauptveranstaltung des Jahres 2004 an: das Netzwerk-, System- und Service-Management-Forum 2004, das wie üblich im November in Königswinter stattfindet.

Entsprechend der genannten Aktualitäten werden wir auf der Basis aktueller Projekte und als Ergebnis speziell für das Forum laufender Analyse-Arbeiten mindestens auf folgende Themen eingehen:

- Back to the roots: wo steht Netzwerk-Management heute, wie können die neuen Anforderungen erfüllt werden
- Security-Management: was brauchen wir, was leisten die Produkte, wie werden sie sinnvoll in vorhandene Lösungen integriert
- Vom End-to-end zum Service-Management: Stand der Technik und Projekterfahrungen
- Management von Geschäftsprozessen: was leistet es, was bringt es
- Benutzertrennung und Secure Networks: Umsetzung einer strukturbrechenden Anforderung in modernen Netzwerken

Eine Reihe der auf dem Forum vorgestellten Analysen und Empfehlungen wird es exklusiv nur auf dem Forum geben, sie werden nicht an anderer Stelle veröffentlicht.

Angesichts der Fülle an neuen Herausforderungen und neuen Themen freue ich mich auf eine spannende und eventuell auch kontroverses Netzwerk-, System- und Service-Management-Forum 2004. Da diese Veranstaltung zu unseren am besten gebuchten Veranstaltungen gehört, sollten Sie zögern, sich rechtzeitig einen Platz zu sichern.

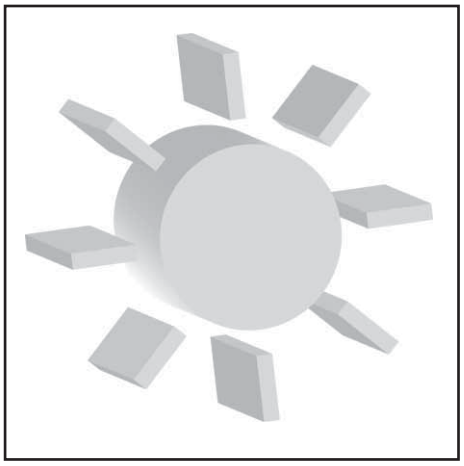
Ihr
Dr. Jürgen Suppan

Top-Event

IP-Telefonie: Intensiv-Evaluierung und IP Betriebsgrundlagen

ComConsult Sommerschule 2004

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Sommerschule 2004

☐ Ich buche das Seminar
Sommerschule 2004
vom 05.07. - 09.07.04 in Aachen
(Preis € 2.290,-- zzgl. MwSt.)

Bitte reservieren Sie für mich ein Zimmer

vom_____bis_____

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

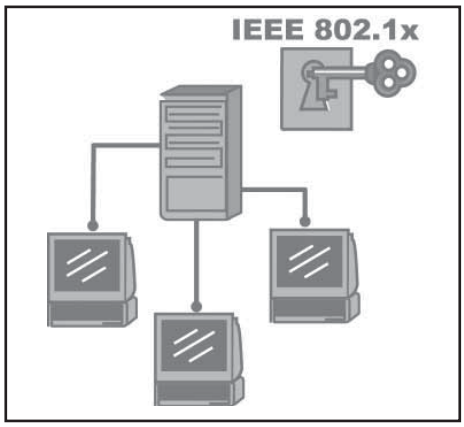
_____ Unterschrift

Neues Seminar

NEU! Sicherheit im LAN mit IEEE 802.1X

Vom 01. bis 02. Juli 2004 veranstaltet die ComConsult Akademie erstmalig ihr neues Seminar „Sicherheit im LAN mit IEEE 802.1x“ im Hilton Hotel in Bonn.

In der Praxis stellt sich häufiger die Aufgabe, in einem gemeinsam genutzten Netzwerk eine Trennung verschiedener Benutzergruppen, die ggf. unterschiedlichen Sicherheitsniveaus zugeordnet werden müssen, vorzunehmen. Ein klassisches Beispiel ist die Unterstützung eines Gastzugangs, der es erlaubt, dass sich Gäste mit ihrem PC an einem „beliebigen“ LAN-Zugang anschließen dürfen und einen Internet-Zugang erhalten. Dass dabei kein Zugriff auf interne Ressourcen gewährt werden darf, ist selbstverständlich. Es muss also an einem geeigneten Punkt im Netz (z.B. direkt am entsprechenden Netzwerk-Port des Access-Switches) geprüft werden, ob es sich bei einem Client um einen Gast oder einen Mitarbeiter handelt. Je nach Ergebnis der Authentifizierung wird ein entsprechend (eingeschränkter) Zugang gewährt und der Verkehr in die eine oder die andere Richtung geleitet. Diese Anforderung kann auch anders formuliert werden: Damit einem Client der Zugang zum Netz gestattet wird, muss der Client bzw. Nutzer sich entsprechend ausweisen. Ein weiterer Bereich,



in dem eine Zugangskontrolle bzw. eine Trennung von Benutzergruppen eine Rolle spielt, ist in industriellen Umgebungen der Aufbau von Netzen, die an einem Ort den Zugriff auf Res-sourcen im Produktions- und im Bürobereich ermöglichen sollen.
So einfach diese Anforderungen auf den ersten Blick wirken, der Teufel steckt im Detail: Damit ein Netzzugang gewährt werden kann, muss sich der Nutzer authentifizieren. Damit sich ein Nutzer authentifizieren kann, benötigt er einen Netzzugang. Die Auflösung dieses „Deadlocks“ und die Spezifikation eines Authentifizierungs-Rahmenwerks für den LAN-Zugang auf Layer 2 ist Inhalt des Standards IEEE 802.1x. Konzeptionelle Basis ist das Extensible Authentication Protocol (EAP), das eine einheitliche Schnittstelle für die Abwicklung unterschiedlichster Authentifizierungsmethoden bietet. Diverse Geräte, die den Standard IEEE 802.1x unterstützen, sind inzwischen verfügbar. Für die Absicherung von WLAN wurde die Verwendung von IEEE 802.1x im Industriestandards Wi-Fi Protected Access (WPA) der Wi-Fi Alliance sowie in IEEE 802.11i festgeschrieben.

Der Aufbau von Netzen mit IEEE-802.1x-Unterstützung ist nicht trivial. Aus vielfältigen Authentifizierungsmethoden und zugehörigen Architekturen ist zu wählen. Die Wirkketten bei IEEE 802.1x können vom Client-Betriebssystem bis hin zum Directory Service reichen. Um eine Position zu IEEE 802.1x und allgemein zu den Themen Zugangskontrolle und Trennung von Benutzergruppen im LAN beziehen zu können und gegebenenfalls sogar eine Umsetzung vorzunehmen, sind umfangreiche Kenntnisse erforderlich. Dieses Seminar liefert das notwendige Rüstzeug.

Referenten sind Dr. Simon Hoff und Dipl.-Ing. Hans Peter Mohn der ComConsult Beratung und Planung GmbH.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sicherheit im LAN mit IEEE 802.1X

☐ Ich buche das Seminar
Sicherheit im LAN mit IEEE 802.1x

__ vom 01.07. - 02.07.04 in Bonn
__ vom 04.10. - 05.10.04 in Bonn

(Preis € 1.390,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Zweitthema

Session Initiation Protokoll bringt 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.

4. SIP Anwendungen und Dienste

4.1 SIP Dienste

SIP Dienste lassen sich aktuell in mehrere Kategorien unterteilen:

- Reine Internet Dienste: Im Regelfall Consumer-orientierte Dienste, die über SIP Registrar Server freie Internet Telefonie für weitere SIP Telefone anbieten, wie z. B. Free World Dialup (www.pulver.com/fwd). Verbindungen zu PSTN-Telefonen funktionieren bei diesen Diensten nur zu kostenfreien Nummern. Die Idee hinter dieser „Verlust-Dienst"-Kategorie ist die Investition in den Aufbau einer starken Marktpräsenz
- Kombinierte PSTN / Internet Dienste: Zusätzlich zu SIP-SIP Telefonie bietet ein Telefonie Provider die Nutzung von PSTN Gateways an, damit Telefonate zwischen SIP- und PSTN-Telefonen geführt und von beiden Seiten initiiert werden können. Dies setzt voraus, dass der Benutzer einen Vertrag mit einem ISP hat, was z.B. bei der Nutzung von DSL Modems im Regelfall gegeben ist.
- Unternehmens-Umfeld: SIP wird für standortübergreifende Verbindungen zwischen Anlagen genutzt, ebenso für Anrufe über PSTN Gateways hinweg. Die PSTN Gateways werden vom Unternehmen und nicht vom Provider betrieben.
- Interne Kommunikation: SIP kann auch zur Anlagen-internen Kommunikation eingesetzt werden, z.B. Trunking zwischen Anlagen, Einbindung von Video oder Kollaboration in eine existierende Telefonie-Lösung oder ähnliches genutzt werden.

SIP bietet außer der Anruf-Signalisierung weitere Basis-Dienste, die zur Anpassung oder Erweiterung von Applikationen genutzt werden können. Aktuell liegt ein hohes Maß an Aktivität auf der Entwicklung von Funktionen zur Anwesenheitsanzeige und für Instant Messaging. Aber auch die Übermittlung zusätzlicher Informationen wie das Senden eines JPEG Bildes oder einer elektronischen Visitenkarte über die SIP Signalisierung sind möglich.

Anwesenheitsanzeige (Presence)

Dieser Basisdienst stellt Informationen über geografische und organisatorische Erreichbarkeit eines Teilnehmers sowie sein aktuelles Endgerät / Medium zur Verfügung:

- Anwesenheit: Listen aktiver Teilnehmer (im Internet und Intranet)
- Lokation: Wo befindet sich ein Teilnehmer: im Büro, unterwegs, im Home Office etc.
- Anrufstatus: Ist der Teilnehmer anrufbereit, belegt, etc.
- Anrufbereitschaft: Ist der Teilnehmer verfügbar, in einer Besprechung, in Urlaub etc.
- Bevorzugtes Medium: Ist die beste bzw. bevorzugte Erreichbarkeit über Text, Sprache, Video oder E-Mail gegeben

Die Anwesenheit eines Teilnehmers kann mit den Aktionen SUBSCRIBE und NOTIFY (siehe hierzu SIP Teil 1, Insider Mai 2004) angezeigt werden: SUBSCRIBE ist eine permanente Überprüfung eines Benutzers B durch einen Benutzer A auf Anwesenheit. Benutzer B wird von dem SUBSCRIBE-Wunsch in Kenntnis gesetzt, erst nach Zustimmung durch B wird das SUBSCRIBE aktiviert: Will der Benutzer Dr. Klöbner den Benutzer Müller-Lüdenscheid erreichen (z. B. um das Thema Badewannenlieferung mit Gummienten-Gimmick zu diskutieren), so startet er ein SUBSCRIBE auf Müller-Lüdenscheid. Herr Müller-Lüdenscheid kommt abends um 20.00 Uhr von einer Dienstreise noch mal in sein Büro und sieht eine Anzeige, dass Dr. Klöbner ein SUBSCRIBE auf ihn aktivieren möchte. Herr Müller-Lüdenscheid stimmt zu, erledigt noch einige Mails und verlässt kurze Zeit später sein Büro. Die SUBSCRIBE Funktion führt nun eine permanente Abfrage durch, ob Herr Müller-Lüdenscheid als Telefonteilnehmer eingeloggt ist. Am nächsten Morgen arbeitet Herr Müller-Lüdenscheid in seinem Büro, Dr. Klöbner ist aber in einer Besprechung. Sobald er von dort zurück ist und sich wieder einloggt, erhält Dr. Klöbner mittels NOTIFY eine Anzeige, dass Herr Müller-Lüdenscheid erreichbar ist – er kann ihn jetzt anrufen, ohne erneut auf der Sprachbox zu landen (siehe Abbildung 4.1).

Instant Messaging (IM)

Im weiteren Sinn könnte IM auch zu den Presence Diensten gezählt werden, da es hierbei um Online Mailfunktionen geht wie

- Online Notizen in beide Richtungen
- Text Chat
- Sprach-Chat
- Verteilung von Web Links verteilen
- Einspielen / gemeinsame Nutzung von Bildern, Audiosequenzen
- Einspielen / gemeinsame Nutzung von Streaming Informationen wie Nachrichten oder Börseninformationen

Vielfach werden sowohl zu Presence-Funktionen als auch zu IM in entsprechenden Anwendungen „Buddy Listen" unterstützt und genutzt, quasi als Cache für die

Teilnehmer, mit denen ein Anwender besonders häufig kommuniziert. Sowohl für IM als auch für Presence gibt es übrigens über die Modellbeschreibung hinaus noch keinen fertigen RFC. Für IM gibt es einen Protokoll-Draft, für Presence bisher nur ein Modell.

Splitten und Wiederholen

SIP kann mittels Splitting (auch als Fork oder Forking bezeichnet) Mediastreams, z.B. einen eingehenden Anruf, parallel in mehrere Streams verzweigen. Damit lässt sich erreichen, dass mehrere Nebenstellen oder Endgeräte (auch PDA, Mobiltelefon) gleichzeitig klingeln. Das erste antwortende Endgerät erhält den Anruf. Fork ist sowohl für Teams als auch für Chef / Sekretär-Schaltungen nutzbar.

Mit weiterer Programmierung können diese Dienste verfeinert werden, z.B.

- Unterschiedlicher Rufton, je nach Anrufer
- Ablehnen aller Anrufe einer bestimmten Person oder rufenden Nummer, ggf. nur außerhalb der Geschäftszeiten
- Rufumleitungen bestimmter Personen auf das private Mobiltelefon, alle anderen auf den Sekretär-Apparat
- Automatischer Rückruf, sobald anwesend
- Ad hoc Konferenzschaltung für alle Teilnehmer einer Liste mit Status „anwesend / verfügbar“
- Anzeige der geografischen Lokation zusammen mit dem Anwesenheitsstatus
- etc.

Erhält ein SIP Server einen Verbindungsaufbau-Request, könnte er mit einer Webseite antworten, auf der weitere Rufnummern (Urlaubsort, Krankheit, Vertretung) als Links eingetragen sind. Der anrufende Teilnehmer kann dann für einen Wiederholungsanruf diese Nummern mit Click and Dial anwählen.

4.2 Kollaboration und andere SIP Anwendungen, die IM und Presence nutzen

Die Integration von Anwesenheits-, IM-, Dokumentenbearbeitung und Telefoniefunktionen schafft erweiterte und neue Möglichkeiten für Kollaboration.

Ein Beispiel: Eine der größten Selbsthilfegruppen für Krebskrankheit in den USA hält regelmäßig Webkonferenzen ab, in denen Hilfeangebote für Patienten und neue Informationen ausgetauscht werden. Mit diesen Konferenzen werden bis zu 14.000 Live-Teilnehmer direkt über Telefon oder über PC erreicht. Heute werden registrierte Mitglieder angerufen, um sich der Konferenz anschließen zu können. Zukünftig könnten sich Teilnehmer mit der SIP Presence Funktion über verschiedenste weitere Geräte wie PDA, Wireless Telefon, GSM-Telefon, PC mittels E-Mail registrieren. Ihr bevorzugtes Teilnehmer-

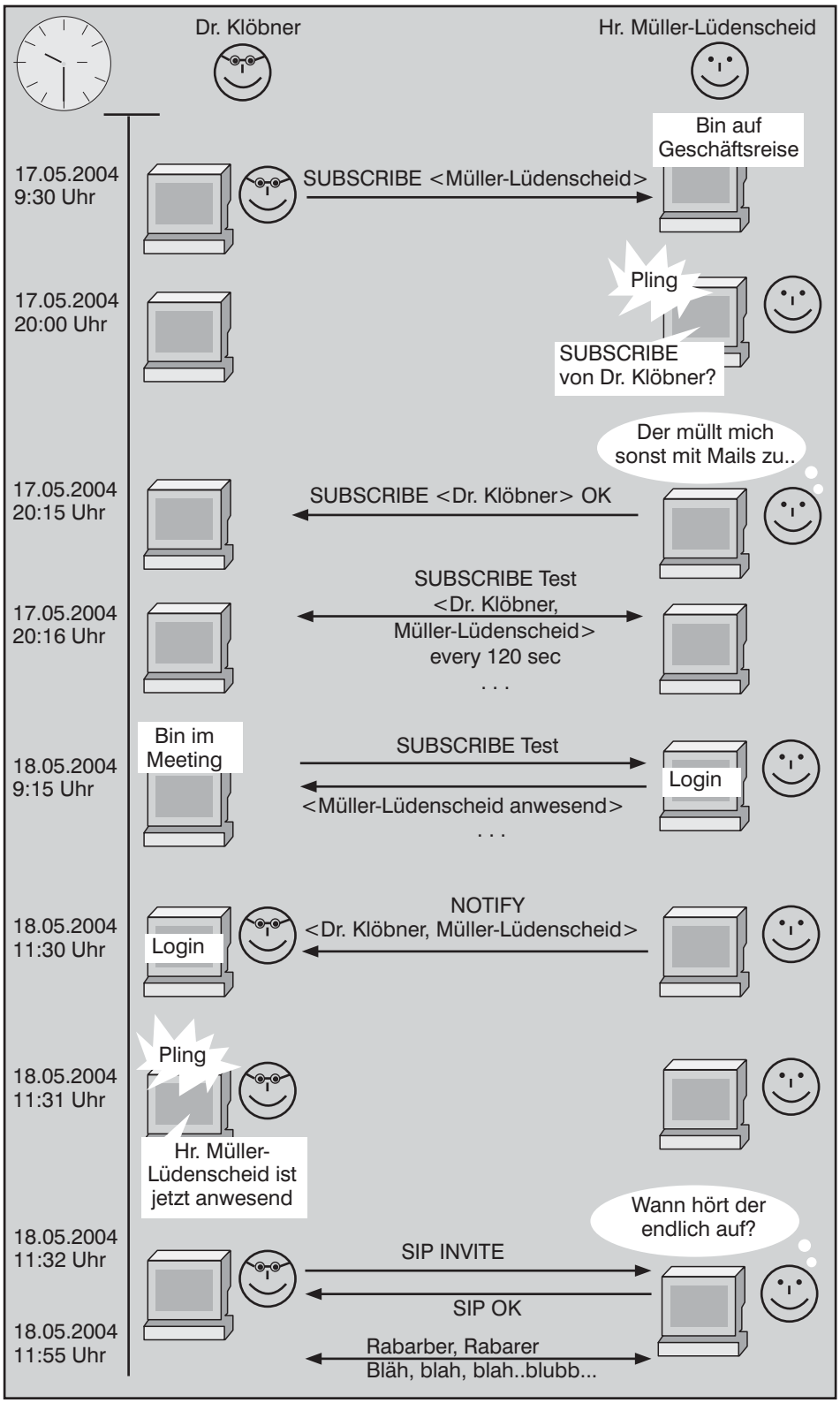


Abbildung 4.1: SIP Anwesenheits-Anzeige

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

Gerät würde bestätigt, eingetragen und zukünftig bei weiteren Konferenzen für eine Benachrichtigung genutzt. Für ein weitergehendes Szenario lässt sich das Selbsthilfe-Beispiel auf technische User Groups übertragen, die zusätzlich mit PR-Aktionen der betreffenden Hersteller gekoppelt werden könnten usw. usw.

Notfall- und Katastrophenabsicherung und die dazugehörigen Eskalationsroutinen können mit SIP und Presence einerseits um Konferenzszenarien erweitert werden, andererseits können alle Eskalationspersonen, deren Anwesenheitsstatus „abwesend / nicht verfügbar“ ist, bei der Eskalation sofort ohne weiteren Zeitverlust übergangen werden.

Kollaboration ist jedoch nicht nur für solche großen globalen Szenarien attraktiv, sondern auch für Projektgruppenarbeit in einem einzelnen Unternehmen: Aus einer Webportal-Oberflläche heraus können Arbeitsgespräche, Projektgruppen-Sitzungen oder Konferenzen mit parallelen „Seitengesprächen“ abgehalten werden, für deren Vorbereitung oder in deren Verlauf die zugehörigen Dokumente über Buddy Listen an alle verteilt und von allen bearbeitet werden.

Eine wichtige und grundlegende Funktion der Anwesenheitsanzeige ist, dass ihre Steuerung letztendlich komplett durch den Benutzer erfolgt, obwohl sie ergänzend durch Voreinstellungsprofile unterstützt werden kann. Der Benutzer entscheidet, wann, wie und für wen er erreichbar sein will.

Verfügbare Produkte mit erweiterten SIP Anwendungen sind beispielsweise Nortels Multimedia Communications Server 5100 (MCS 5100) und OpenScape von Siemens.

Der MCS 5100 unterstützt in der aktuell verfügbaren Version 2 bis zu 10.000 Benutzer und verbindet Telefonie, Mobility und Personalisierung mit den SIP-basierten Diensten Konferenzschaltung, Bildtelefonie und Kollaboration (siehe das Einsatz-Szenario in Abbildung 4.2).

Er beinhaltet einen H.323 Gatekeeper und ein H.323 / SIP Signalisierungs-Gateway, ebenso eine Gateway-Schnittstelle (MCP-Trunk, QSIG und DPNSS) zur Nortel-eigenen Signalisierung, so dass SIP Telefone, H.323 Endgeräte und Nortel-Telefone integriert werden können.
Funktionen sind z.B:

- Multimedia: Instant Messaging, Video Telefonie, Telefonie, Collaboration, Web Co-Browsing

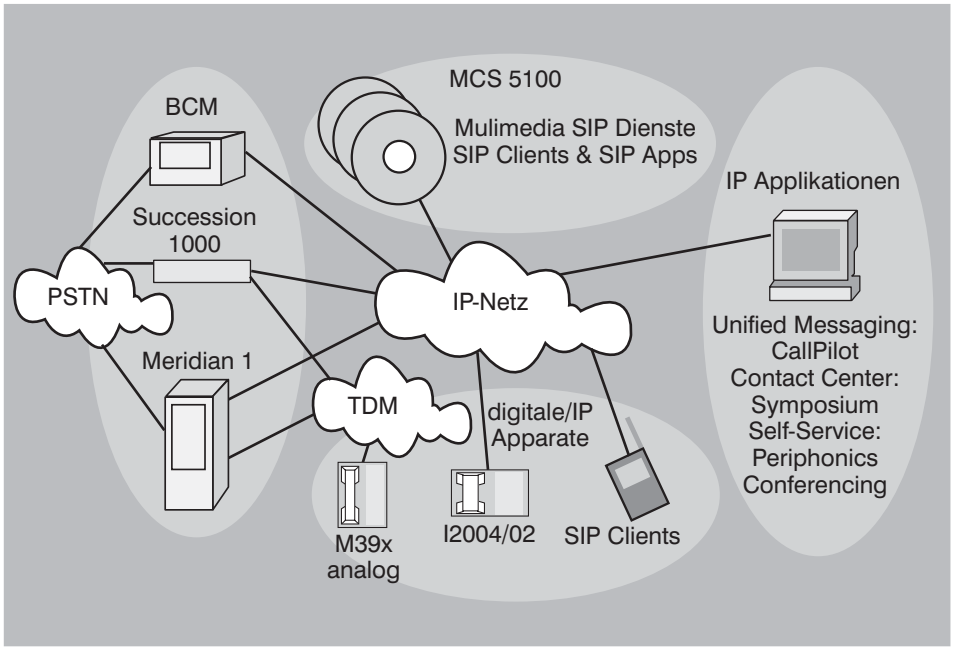


Abbildung 4.2: MCS 5100 Einsatzszenario

- Personalisierung: Rufweiterleitung, Persönliches Rufmanagement (Verzeichnisse, Verzeichnis-Anwahl, Anruf-/Wahlwiederholungsliste), Anwesenheitsmanagement

- Mobilität: Hot-Desk, Find-me / Guide-me (simultane und parallele Anrufe)

OpenScape ist eine Siemens-Entwicklung für konvergente Kommunikation auf der Basis des Microsoft LCS (Live Communication Server) zur Integration von TK mit typischen Groupware-Anwendungen wie:

- Erreichbarkeit (bin da, bin im Meeting, bin in Urlaub etc.),
- Status (frei, belegt, ausgeloggt),

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

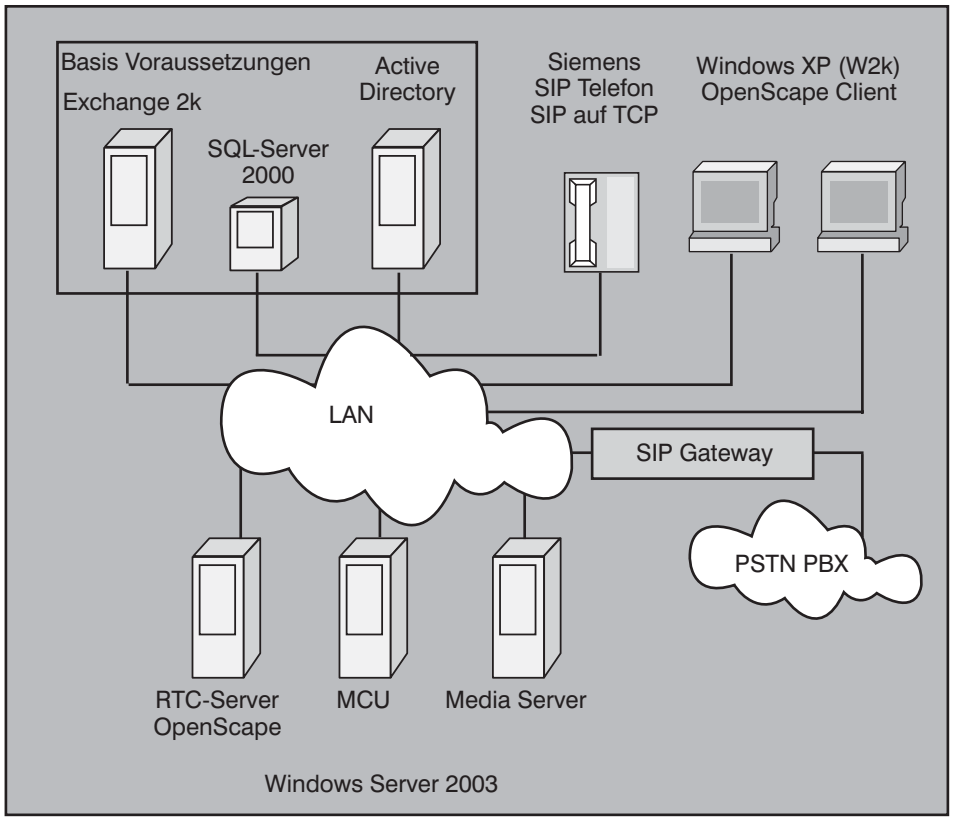


Abbildung 4.3: OpenScape Einsatzszenario

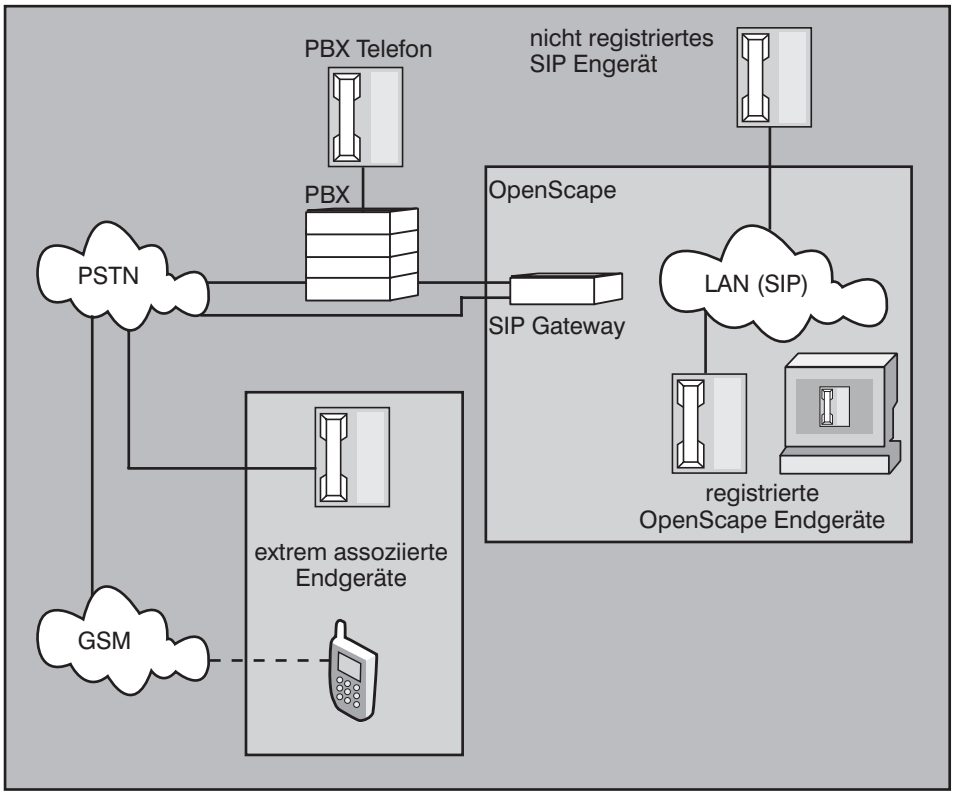


Abbildung 4.4: OpenScape, SIP- und non-SIP-Geräte

- Instant Messaging (IM),
- Hauptkontakte („Buddy Liste“),
- Vorzugstelefonliste (MyCalls)

für Arbeitsgruppen oder Unternehmensabteilungen. Verfügbar ist die Version 1, sie unterstützt bis zu 500 Benutzer. OpenScape ist zu den Workflow-Lösungen zu rechnen und erweitert das Erreichbarkeitsmodell dadurch, dass verschiedenste Kommunikationsmedien und -geräte eingebunden werden – und dazu gehören auch Telefone. Es beinhaltet ein „Personal Portal“ und ein „Community Portal“ für Teams oder Arbeitsgruppen. Eine Übersicht der OpenScape Komponenten zeigt Abbildung 4.3.

Das „Personal Portal“ dient der Personalisierung typischer Anrufbearbeitungs-Funktionen oder Konfigurierung von Rufumleitungs-Regeln wie

- Festlegen eines bevorzugten Telefons
- Umleitung auf Voice-Mail
- Umleitung auf Instant Messaging
- Durchschaltung
- Umleitung auf eine andere Rufnummer
- etc.

Telefonpartner, die häufig angerufen werden, können über eine separate „My Calls“-Liste schnell angewählt werden. Andere OpenScape-Benutzer können durch Eingabe ihrer E-Mail-Adresse der Kontaktliste „My Contacts“ hinzugefügt werden. Für sie erfolgt dann eine Statusanzeige ihrer Erreichbarkeitsmedien (per Telefon, Instant Message, E-Mail) und ihres Erreichbarkeitsstatus (kurz abwesend, Meeting, Urlaub, Dienstreise). Der Aufbau von Konferenzen und Dokumentbearbeitungs-Sessions kann per Menü angewählt werden. Der Vorteil von „My Contacts“ im Vergleich zu „My Calls“ besteht darin, schon vor der Anwahl über den Status der Kommunikationspartner informiert zu sein und diese dann gezielt durch Auswahl des entsprechenden Mediums ansprechen zu können.

Das „Community Portal“ ermöglicht Gruppenaktionen. Dies geschieht durch die Definition so genannter „Collaborations“ unter einem entsprechenden Gruppennamen anstelle eines Benutzernamens. Per Mausklick auf die „Collaboration“ lassen sich dann Funktionen für die ganze Gruppe aktivieren:

- Konferenz,
- Dokumentenbearbeitung.

Für eine Implementierung von OpenScape sind folgende Microsoft-Produkte Voraussetzung

- Windows 2003 Server, hier insbesondere der LCS als Peer-to-Peer Communication Engine
- Active Directory Service (ADS)
- Exchange 2000
- SQL Server 2000

OpenScape nutzt wie auch der LCS das SIP-Protokoll (wegen der Microsoft Kompatibilität über TCP, nicht UDP!). Um Endgeräte aus dem öffentlichen Netz oder PBX-Endgeräte (z.B. CorNet-Telefone) zu integrieren, wird ein SIP-Gateway benötigt (dieses ist noch nicht angekündigt). Solche Geräte werden als „associated Devices“ angezeigt. Dies können zum Beispiel Mobiltelefone, SOHO-Telefone oder auch CorNet-IP-Telefone einer HiPath-Anlage etc. sein. Eine Übersichts-Grafik ist in Abbildung 4.4 dargestellt.

4.3 Microsoft und SIP

Microsoft verstärkt seit mehreren Jahren die Integration von Sprache in seine Echtzeit-Kommunikations-Funktionen im Rahmen der Netzwerk- und Betriebssystem-Software. War das Protokoll der Wahl bei Netmeeting und TAPI noch H.323, so ist mit dem Microsoft Live Communication Server (LCS, früher RTC Server) und Windows Messenger der Schwenk auf SIP erfolgt. Der Windows Messenger ist als professioneller Echtzeit-Dienst mit der XP Betriebssystemsoftware gebündelt und wurde für den Consumer Bereich durch den MSN Messenger ergänzt, der um einige „Spaßfunktionen“ für private Benutzer wie z.B. Spiele erweitert ist. In diesem Beitrag beschränken wir die Betrachtung auf den Windows Messenger. Werden der .NET Messenger und Exchange IM eingesetzt, so läuft die Session über TCP, wird ein SIP Proxy Server eingesetzt, so sind TCP, UDP oder SSL einstellbar.

Der Windows Messenger unterstützt die typischen SIP Dienste:

- Anwesenheitsanzeige (SIP REGISTER, SUBSCRIBE, NOTIFY)
- Instant Messaging
- Sprache und Video (über SIP, nicht H.323)
- Application Sharing und Whiteboard
- Dateitransfer

In den neueren Messenger Versionen werden nicht nur PC-PC AV Streams sondern auch Audiokommunikation zwischen PC und Telefonen unterstützt. Zur Verbreitung von AV-Diensten im Internet auf der Basis von Microsoft Software führt Microsoft eine Provider-Zertifizierung durch, die Einsatz-Szenarien wie das nachfolgend beschriebene unterstützt.

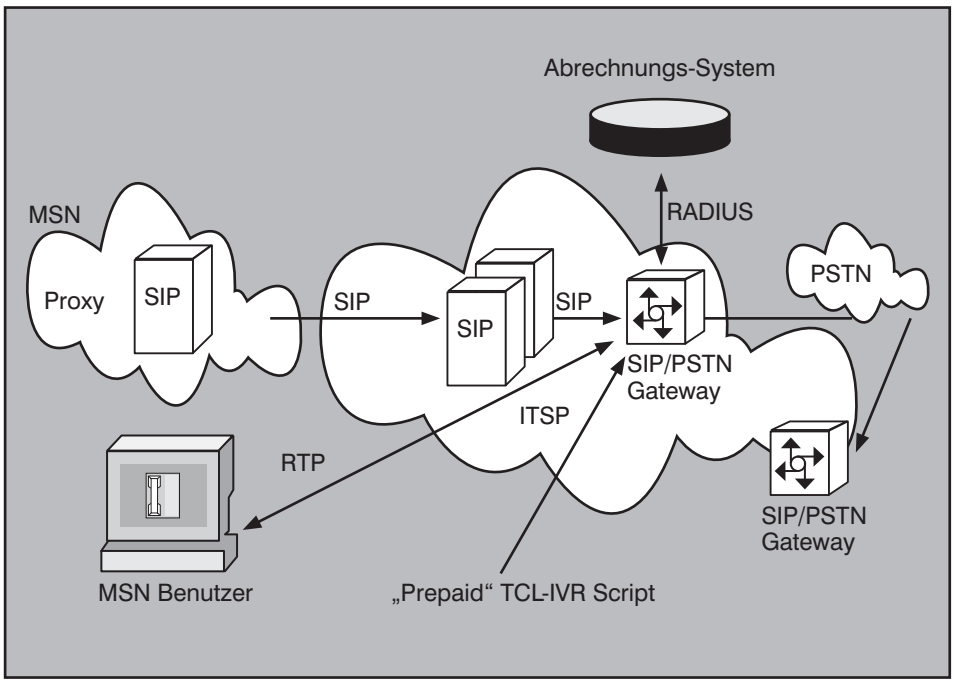


Abbildung 4.5: Prepaid Einsatz-Szenario mit dem Windows Messenger

Einsatz-Szenario

Für einen ITSP Dienst, der im SOHO Bereich genutzt wird, sind folgende Komponenten erforderlich:

- Der Windows Messenger (.NET Messenger), der auf den PC‘s installiert ist
- Ein Passport Server (inkl. Backup !), der im Providernetz implementiert ist
- Eine SSH Verbindung zwischen PC‘s und Passport Server
- Ein bzw. mehrere MS SIP Proxy Server im internen Netz (MSN), die Anrufe ins PSTN zu den ITSP‘s routen
- Eine IPSec VPN Verbindung zwischen dem internen Netz (MSN) und dem ITSP
- Ein bzw. mehrere SIP Proxy Server im ITSP Netzwerk, die Anrufe ins PSTN zu den SIP Gateways routen
- SIP / PSTN Gateways mit Anschaltung ans PSTN, die Anrufe zum PSTN terminieren (Call Termination)

Ein PC – Telefon Anruf mit Prepaid Abrechnung sieht dann so aus (siehe auch Abbildung 4.5): Der Benutzer loggt sich mit dem Messenger Client beim MSN Voice.Net Dienst mittels Benutzername und Passport ID ein. Es erscheint ein Prompt mit einer Liste lokaler ITSP‘s für PC-to-Phone Anrufe. Der Prompt wird über die Passport Datei generiert. Der Benutzer entscheidet sich für einen bestimmten Anruf („Make a Phone Call“ Launch). Wenn der Benutzer die Nummer anklickt / wählt, routet der MS SIP Proxy Server den Anruf zum SIP Proxy Server des gewählten ITSP‘s. Der ITSP SIP Proxy Server routet den Anruf zum entsprechenden SIP/PSTN Gateway und somit ins PSTN.

Anforderungen an den ITSP sind:

- Zertifizierung durch MS mit dem MS-eigenen Testnetz; d.h. der ITSP muss in der Lage sein, mit dem MSN User Provisioning Modell zusammenzuarbeiten
- Der ITSP muss einen IPSec VPN Tunnel zu MSN Netzwerken betreiben können, um eine gesicherte Signalisierung zwischen MSN und ITSP zu realisieren
- Unterstützung von G.711 oder G.723.1 (!) Codec beim ITSP
- Der ITSP muss Passport User ID‘s (PUID) aus der SIP Signalisierung entnehmen und die PUID mit der Abrechnung für einen bestimmten Benutzer mappen können
- Einfügen eines Record Route Headers durch den ITSP SIP Proxy Server
- Garantiertes maximales one-way Delay von 150 ms

Fortsetzung folgt!

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

Studie des Monats

Aktueller Report: Windows Server 2003 - Active Directory und IP-Management

Der soeben bei der ComConsult Technologie Information GmbH erschienene Report beschreibt ausführlich alle Planungs- und Realisierungsaspekte einer Active-Directory-Infrastruktur basierend auf Windows Server 2003 und Active Directory Version 2. Es werden das vollständige Themenspektrum von der notwendigen IP-Infrastruktur hinsichtlich dynamischem DNS in Kombination mit DHCP sowie die Notwendigkeit von WINS, die logische und physikalische Planung des Active Directory bis hin zur Standardisierung der Clientwelt über Gruppenrichtlinien behandelt. Darüber hinaus werden mögliche Migrationswege in die neue Welt beschrieben und bewertet. Abschießend erfolgt dann eine Betrachtung der Möglichkeiten zur Konsolidierung und zur Kopplung verschiedenster Verzeichnisdienste.

Gruppenrichtlinien im Active Directory

Mithilfe der Gruppenrichtlinien von Windows 2000, Windows 2003 und Windows XP lassen sich über 600, seit Windows 2003 sogar über 900 verschiedene Einstellungen vornehmen. Damit steht ein mächtiges Werkzeug zur zentralen Administration und zur Standardisierung von Clients zur Verfügung, dessen Grundsätze im Folgenden kurz beleuchtet werden.

Zunächst wird bei jedem Gruppenrichtlinienobjekt zwischen Einstellungen für den Benutzer (Benutzerkonfiguration) Einstellungen für den Computer (Computerkonfiguration) unterschieden.

- Computerkonfiguration
  Hier sind alle Richtlinien enthalten, die der Konfiguration des Computers dienen. Diese Richtlinien gelten für alle Benutzer eines Windows 2000/2003/XP Computers, und werden beim Start des Computers angewendet.
- Benutzkonfiguration
  Hier sind alle Richtlinien enthalten, die auf einen Benutzer angewendet werden, sobald dieser sich anmeldet.

Sollte es einen Konflikt zwischen den Einstellungen in der Computer- und der Benutzerkonfiguration geben (manche Einstellungen sind sowohl in der Computer- als auch in der Benutzerkonfiguration definierbar), so besitzt die Computerkonfiguration die höhere Priorität.
Die nachfolgende Aufstellung vermittelt einen Überblick, in welchen Bereichen über Gruppenrichtlinien Einstellungen vorgenommen werden können.

Administrative Vorlagen

Hier können registry-basierte Einstellungen vorgenommen und angepasst werden. Die Arbeitsumgebung an Windows 2000/2003/XP Rechnern kann mit Hilfe der administrativen Vorlagen zentral festgelegt werden und ist verbindlich.
So können z.B. das Erscheinungsbild und die Eigenschaften des Desktops und der Systemsteuerung verändert werden, es kann der Taskmanager deaktiviert oder die Verwendung eines kennwortgeschützten Bildschirmschoners vorgeschrieben werden. Alle Einstellungen werden in die Registry in den computer- oder benutzerspezifischen Teil eingetragen. Administrative Vorlagen sind als „ADM-Dateien“ gespeichert.

Windows 95/98 und Windows NT verwenden ebenfalls ADM-Dateien. Diese ADM-Dateien sollten nicht unbesehen übernommen werden, da sich unter Windows 2000/2003/XP die Benennung oder der Ort einiger Registrierungsschlüssel geändert hat.

Sicherheitseinstellungen

Hier können sicherheitsrelevante Definitionen wie z.B. Einstellungen bezüglich des Ereignisprotokolls oder der Systemdienste vorgenommen werden. Zu den Sicherheitseinstellungen zählen auch die so genannten Kontorichtlinien, über die Einstellungen bezüglich der von den Benutzern verwendeten Kennwörter sowie Vorgaben für die Kerberos-Authentifizierung vorgenommen werden.

Die Kontorichtlinien sowie die Richtlinien öffentlicher Schlüssel gelten immer für die gesamte Domäne und nicht nur für einen oder mehrere Container. Diese sind wirkungslos, wenn sie einer OU zugewiesen werden.

Die Kontorichtlinien setzten sich zusammen aus den Kennwortrichtlinien, Kennwortsperrungsrichtlinie und der Kerberos-Richtlinie.

Skripte

Über diesen Punkt erfolgt die Zuweisung von Skripten, die beim Starten oder Herunterfahren des Computers und beim An- oder Abmelden des Benutzers ausgeführt werden. Dabei sind sowohl Skripte des Windows Scripting Hosts als auch der command-Shell (cmd.exe) möglich.

Softwareinstallation

Hier kann die richtlinienbasierte Installation von Software (Zuweisen und Veröffentlichen) eingerichtet werden. Die Installation kann dabei zwingend stattfinden, oder erst dann, wenn der Benutzer es wünscht.

Internet-Explorer-Wartung

Über diesen Punkt erfolgt die Verwaltung der Internet-Explorer-Einstellungen. Dabei kann es sich zum Beispiel um die anzuzeigende Startseite, die Verbindungskonfiguration oder die Favoriten handeln.

Remoteinstallationsdienste

Hier erfolgen die Einstellungen für RIS (Remote Installation Service) zur (weitest gehenden) automatischen Installation des Betriebssystems über das Netzwerk.

Ordnerumleitung

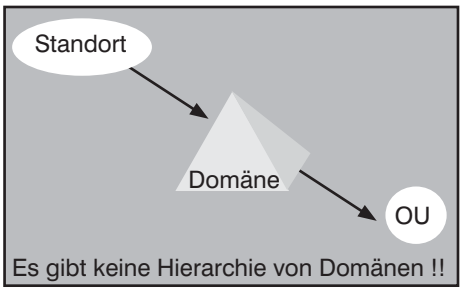
Über die Ordnerumleitung können bestimmte Ordner einer Windows-Arbeitsstation auf einen Server im Netzwerk umgeleitet werden. Als Folge daraus stehen beispielsweise den Benutzern unabhängig davon, an welchem PC sie sich anmelden, immer seine „Eigene Dateien“ und seine Favoriten zur Verfügung.

Anwendung von Gruppenrichtlinien

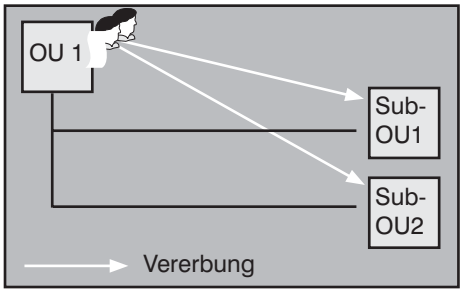
Gruppenrichtlinienobjekte können mit den folgenden Containern verknüpft werden und werden nach Anwendung der lokalen Einstellungen in genau dieser Reihenfolge auch abgearbeitet:

- Standorte (Sites)
- Domänen
- OUs

Dabei findet in der Standardeinstellung eine Vererbung der über das Gruppenrichtlinienobjekt vorzunehmenden Einstellungen statt. Wird z.B. auf Domänenebene ein Gruppenrichtlinienobjekt zugeordnet,



so gelten die getroffenen Einstellungen für alle Container in dieser Domäne, also für die OUs, Benutzer- und Computerkonten.
Die Abbildung stellt die Vererbung dar. Der Organisationseinheit „OU1“ ist ein Gruppenrichtlinienobjekt zugeordnet. Die Organisationseinheiten „Sub-OU1“ und „Sub-OU2“ sind untergeordnete OUs, auf die durch die Vererbung das Gruppenrichtlinienobjekt automatisch angewendet wird.



Die Gruppenrichtlinienobjekte, die als letztes angewendet werden (die also dem jeweiligen Benutzer- oder Computer-Objekt „am nächsten gelegen“ sind), besitzen standardmäßig die höchste Priorität. Einstellungen, die also beispielsweise auf Domänenebene vorgenommen werden, können von Einstellungen auf niedrigeren Ebenen überschrieben werden. Daraus resultiert das folgende Verhalten:

- Das lokale Gruppenrichtlinienobjekt besitzt die niedrigste Priorität.
- Die mit dem Standort verknüpften Gruppenrichtlinienobjekte werden als erstes angewendet.
- Danach werden die Gruppenrichtlinienobjekte, die mit der Domäne verknüpft sind, angewendet.
- Nun kommen die mit den OUs verknüpften Gruppenrichtlinienobjekte zum Zuge. Innerhalb der OU-Hierarchie wird dabei Ebene für Ebene abgearbeitet, bis die OU erreicht ist, in der sich das betreffende Benutzer- oder Computer-Objekt befindet.

Auf diese Weise ist es möglich, Gruppenrichtlinien für jeden Zweck bereitzustellen. Einstellungen, die mehrere Container betreffen, lassen sich dabei einfach auf einer der darüber liegenden Container-Ebenen vornehmen.

Das Verhalten der Vererbung lässt sich – falls gewünscht oder erforderlich – mit Hilfe der Einstellungen

- Richtlinienvererbung deaktivieren
- Richtlinienvererbung erzwingen

beeinflussen.

Richtlinienvererbung deaktivieren

Sowohl mit dem Active Directory Verwaltungsprogramm für Standorte (Active Directory Standorte und Dienste) als auch mit dem Active Directory Verwaltungsprogramm für Domänen und OUs (Active Directory Benutzer und Computer) kann die Gruppenrichtlinienvererbung deaktiviert werden. Dabei kann für jeden Container bestimmt werden, ob die mit darüber liegenden Containern verknüpften Gruppenrichtlinienobjekte auch für diesen Container Anwendung finden sollen.
Bei einer Deaktivierung findet ab diesem Container keine Vererbung übergeordneter Gruppenrichtlinien mehr statt.
Ein selektives Deaktivieren der Richtlinienvererbung ist nicht möglich. Nach dem Deaktivieren werden alle mit darüber liegenden Containern verknüpften Gruppenrichtlinienobjekte abgeblockt, solange sie nicht über die Funktion „Kein Vorrang“ priorisiert wurden.

Richtlinienvererbung erzwingen

Mit den oben genannten Verwaltungsprogrammen kann außerdem die Richtlinienvererbung erzwungen werden, indem die Richtlinienoption „kein Vorrang“ gewählt wird. Bei Aktivierung erhält das gewählte Gruppenrichtlinienobjekt auf jeden Fall Anwendung in allen darunter liegenden Containern. Die Richtlinienvererbung wird selbst dann in unterliegenden Containern erzwungen, wenn für diese die Richtlinienvererbung deaktiviert ist. Einstellungen aus einer „erzwungenen“ Richtlinie („Kein Vorrang“) können nicht mehr von später angewendeten Gruppenrichtlinien überschrieben werden.
Das Erzwingen der Richtlinienvererbung kann selektiv erfolgen.

Die Autoren dieses hochaktuellen Reports sind ein Team der ComConsult Beratung und Planung GmbH.

Schwerpunktthema

Design von „Voice-ready“ Netzen

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.

Für den Betrieb von Sprache über „Datennetze“ oder anders ausgedrückt den Betrieb von Sprache über Ethernet und IP Netzwerke müssen einige Grundvoraussetzungen hinsichtlich Verfügbarkeit und Gesamtleistung gegeben sein, die wir vorab behandeln. Können diese als gegeben oder mittels Migration erreichbar vorausgesetzt werden, sind einerseits die Fragen zum Einsatz der Endgeräte und TK-Anlagen bzw. TK-Server zu klären, andererseits für deren Anbindung geeignete Netzwerkkomponenten zu beschaffen oder hochzurüsten.

1. Verfügbarkeit

Sobald der Betrieb von Sprachanwendungen über ein IP / Ethernet Netzwerk zur Debatte steht, ist in den meisten Fällen von einer Hochverfügbarkeits-Anforderung an das Netzwerk auszugehen. Wird Telefonie über IP betrieben, unterliegt die Verfügbarkeit allen aus Datennetzen bekannten Störfallursachen: Hardware-Fehler, Software-Fehler und komplexere Fehlersituationen aufgrund wechselseitiger Abhängigkeiten. Für eine ausführliche Beschreibung möglicher Störfallursachen sowie die Eingrenzung von Störfällen durch Layer-2-Kopplung und Layer-3-Kopplung als Betriebstechnik verweisen wir auf den Technologie Report „Designvarianten Lokaler Netzwerke im Vergleich“.

Eine Ausfallsituation bedeutet, eine mehr oder weniger große Benutzergruppe kann nicht mehr telefonieren, was von den meisten Anwender und Betreibern maximal für einen Zeitraum von Sekunden bis wenigen Minuten akzeptiert wird. Der gelegentlich auftauchende Vorschlag, das GSM Mobiltelefon sei doch eine implizite Backuplösung, da die meisten Mitarbeiter heute über ein solches Telefon verfügen, trägt jedoch nicht oder nur bei sehr kleinen Standorten: In einer Mobilfunkzelle können nur wenige parallele Anrufe bearbeitet werden! Wollten die Benutzer einer kompletten Etage gleichzeitig von Festnetz-Telefonie auf Mobilfunk-Telefonie umswitchen, würde das Mobilfunknetz zusammenbrechen. Daher muss für alle mittleren bis großen Standorte eine ausreichende Verfügbarkeit mittels Netzwerk-Design und Auslegung der TK-Komponenten sichergestellt werden.

1.1 Kaskadierung, Redundanz und Verfügbarkeit

Zum Vergleich einer klassischen TK-Lösung und einer TK-Lösung über IP treffen wir die nachfolgenden Annahmen:

- V (Telefon): „Unintelligente“ Telefone fallen sehr selten aus
  Annahme: 4 Stunden in 10 Jahren
  V = 1- 4 / (10 * 365 * 24) = 99,995 %
- V (Anlage)
  Annahme: 1 Stunde im Jahr
  V = 1- 1 / (365 * 24) = 99,989 %
- V (PSTN-Netz):
  Annahme: 2 Stunden im Jahr
  V = 1- 2 / (365 * 24) = 99,977 %

Dies führt bei der in Abbildung 1.1 gezeigten typisch sternförmigen Anbindung zu folgender Gesamtverfügbarkeit:

- Gesamtverfügbarkeit V =
  V (Telefon) * V (Anlage) * V(PSTN)
  V = 0,99995 * 0,99989 * 0,99977
  V = 99,961 %

Dies entspricht **3,40 Stunden** Ausfallzeit pro Jahr.

Bei IP Telefonie ist das Telefon ans normale Datennetz angeschaltet. Die Kaskade verläuft im Regelfall vom Telefon mit Ethernet-Anschluss über einen Etagenswitch an einen Gebäudeswitch, von dort über eine RZ-Zugangsswitch in das Rechenzentrum an den Telefonie-Server und für externe Gespräche über ein Gateway ins weltweite PSTN-Netz (siehe Abbildung 1.2).

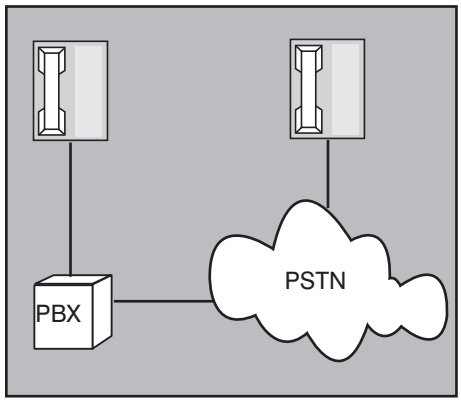


Abbildung 1.1: Klassische TK-Schaltung

Wir nehmen hier bei Herstellern mit gutem Qualitätsniveau folgende Einzelverfügbarkeiten an:

- V (Telefon):
  Annahme: 2 Stunden im Jahr
  V = 1- 2 / (365 * 24) = 99,977 %
- V (Switch) = V (Etagenswitch) =
  V (Gebäudeswitch) = V(RZ-Switch)
  Annahme: 2 Stunden im Jahr
  V = 1- 2 / (365 * 24) = 99,977 %
- V (Server) = V (Gateway):
  Annahme: 3 Stunden im Jahr
  V = 1- 3 / (365 * 24) = 99,966 %
- V (PSTN-Netz):
  Annahme: 2 Stunden im Jahr
  V = 1- 2 / (365 * 24) = 99,977 %

Dies führt bei der gezeigten Schaltung zu folgender Gesamtverfügbarkeit:

- V = V (Telefon) * V^3 (Switch) *
  V (Server) * V (Gateway) * V (PSTN)
  V = 0,99977 * 0,999773 * 0,99966 * 0,99966 * 0,99977
  V = 99,82 %

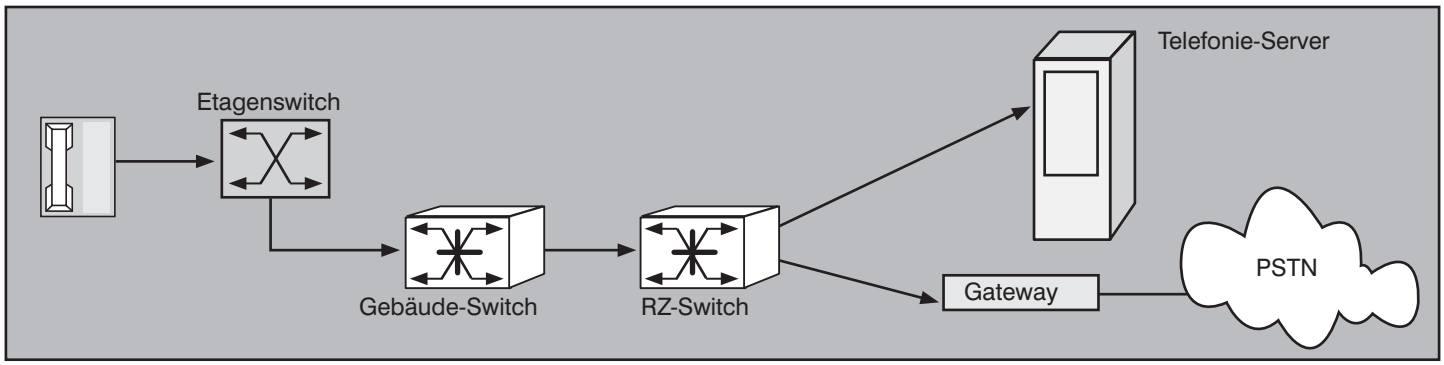


Abbildung 1.2: Telefon-Anschaltung bei IP Telefonie

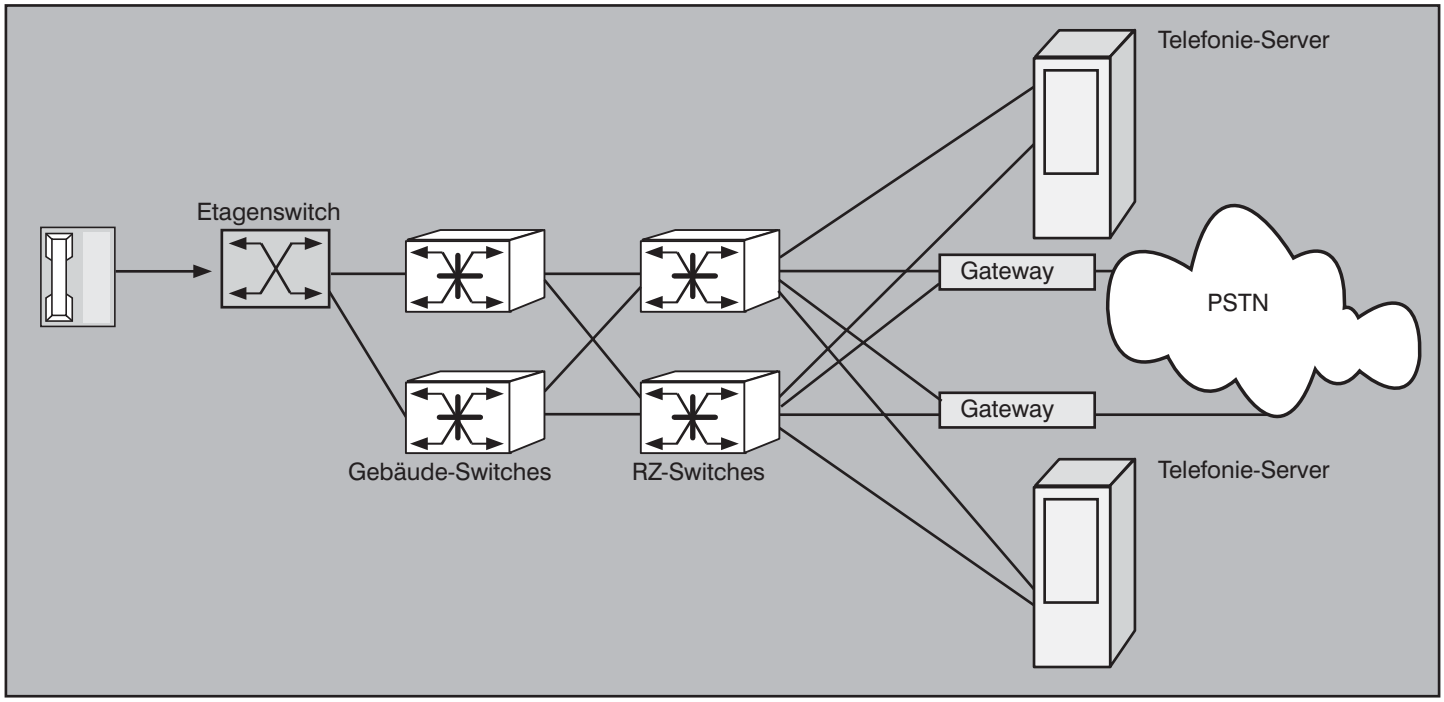


Abbildung 1.3: Telefon-Anschaltung bei IP Telefonie mit redundantem Kernnetz, TK-Server und TK-Gateway

Dies entspricht 15,99 Stunden Ausfallzeit pro Jahr, was im Vergleich zur klassischen Schaltung unakzeptabel ist. Daher muss für Server, Gateway und das Netzwerk eine fehlertolerante Konfiguration gewählt werden, wie z.B. in Abbildung 1.3 gezeigt. Die redundante Auslegung ab dem Etagenswitch-Uplink inklusive Telefonie-Server und Gateway ergibt die nachfolgend berechneten verbesserten Verfügbarkeitswerte.

- Die Verfügbarkeit VR einer Redundanz-Schaltung zweier Komponenten der Verfügbarkeit V1 und V2 berechnet sich aus 1- Redundanz-Ausfallwahrscheinlichkeit (AR)
  VR = 1 - AR mit AR = A1 * A2
  und A1 = 1 - V1
  und A2 = 1 - V2
  VR = 1 - (1 - V1) * (1 - V2)

- Es gilt wiederum:
  V (redund. Gebäudeswitch)
  = V (redund. RZ-Switch)
  = V (redund. Server)
  = V (redund. Gateway)

- Dies führt zu der Gesamtverfügbarkeit V = V (Telefon) * V (Etagenswitch) * V^2 (redund. Switch) * V^2 (redund. Komponente) * V (PSTN-Netz)
  V =
  0,99977 * 0,99977 * (1-(1-0,99977) * (1-0,99977))² * (1-(1-0,99966) * (1-0,99966))² * 0,99977
  V = 0,99931
  V = 0,9999997 für den redundanten Kernbereich

Dies entspricht 6,03 Stunden Ausfallzeit pro Jahr für die Gesamtschaltung, jedoch nur **0,2 Minuten** für den redundant ausgelegten Kernbereich: Gebäude-Switches, RZ-Switches, TK-Server und TK-Gateway! Werden weitere TK-Applikationen wie Unified Messaging, Call Center oder CTI mit zusätzlichen Servern implementiert, so sind diese Server bei entsprechend hohen Verfügbarkeitsanforderungen gleichermaßen in das gezeigte Redundanzkonzept einzubeziehen.

1.2 Redundanzauslegung von Komponenten

Zur Redundanz-Auslegung gehören auch Maßnahmen für eine einzelne Netz- und TK-Komponente. Betrachten wir zuerst die Netzkomponenten, dann TK-Anlagen / TK-Server und Gateways.

Netzkomponenten
(Switches und Router)

Die meisten Redundanzmaßnahmen beziehen sich auf modulare Geräte, da ein Workgroup-Switch als Single Point of Failure (SPoF) aufgrund der begrenzten maximalen Anzahl Anschlussports meistens so wenige Endgeräte betrifft, dass hier auf aufwändige Redundanzmaßnahmen verzichtet wird. Mögliche Absicherungen sind:

- Zweites Gerät
- Redundante und mittels USV unterbrechungsfreie Stromversorgung, mindestens Anschaltung an mehrere Stromkreise (bei Workgroup Switches gegebenenfalls abwechselnd, bei modularen Switches je Switch)
- Redundante lastverteilte PSU, redundante Lüfter (Fan) soweit möglich
- Redundante CPU / CPU‘s
- Passive oder geteilte Backplane
- Bei stackbaren Workgroup Switches: redundante Stackverbindung
- Hot Plug Fähigkeit für alle Module
- Parallelschaltung eines zweiten gleichausgelegten Gerätes
- Einsatz von Redundanz-Schaltungen / Redundanzverfahren mit automatischer Fehlerumschaltung (Failover)
- Blockierungsfreie Auslegung der Interface-Module
- Regelmäßiges Konfigurations-Backup

TK-Server / TK-Anlagen

Sofern Chassis-Systeme oder Shelf-Systeme als TK-Anlagen eingesetzt werden, sind ganz ähnliche Redundanzmaßnahmen wie für modulare Switches verfügbar. Sofern Softswitches eingesetzt werden, sind Redundanzmaßnahmen wie für Datenserver anwendbar. Teilweise werden jedoch nicht alle möglichen Server-Redundanzen von der Software des TK-Herstellers unterstützt bzw. sind für die gebündelte Auslieferung von Hardware und Software nicht freigegeben:

- Mehrfach-CPU
- Versorgung mit USV
- Plattenauslagerung auf RAID Systeme (sofern unterstützt)
- Mehrere Netzadapter (NIC‘s; sofern unterstützt)
- Anschaltung des Servers an mehr als eine Netzkomponente
- Aufbau von Server-Clustern oder Hunt-Gruppen (sofern unterstützt)
- Überwachen von Switchports, an denen TK-Server angeschaltet sind
- Vorhalten von TK-Applikationen, Benutzerprofilen und Gatekeeper-Funktion gedoppelt auf mehreren TK-Servern
- TK-Serveranschaltung an ein separates Backend-Netz (RZ-Netz)
- Konfiguration eines separaten logischen Subnetzes für TK-Server

Manche Hersteller unterstützen den lastverteilten Betrieb redundanter TK-Server (z.B. Cisco; Alcatel ab dem nächsten Release), andere lediglich hot standby. Teilweise kann ein Backup Server nicht „einfach alle Sessions des Default Servers übernehmen“, sondern für eine hot standby Redundanz müssen alle TK-Benutzer doppelt definiert, d.h. explizit einem Primary und einem Secondary Server zugeordnet werden.

Gateways

Die möglichen Redundanzfunktionen hängen von der eingesetzten Gateway-Komponente ab:

- PC/Server mit Gateway-Software: die unter „TK-Server“ aufgeführten Maßnahmen
- Standalone Komponente: vielfach werden keine besonderen Redundanzmaßnahmen unterstützt, in diesem Fall muss das Gateway gedoppelt oder bei mehreren Gateways an einem Standort als N+1 Redundanz ausgelegt werden.
- Layer-3 Switch oder Router mit Gateway-Software: die unter „Netzkomponenten“ aufgeführten Maßnahmen

Nachfolgend geben wir ein einfaches Beispiel für die Redundanz-Auslegung von TK-Servern und PSTN-Gateways. Wir nehmen an, ein TK-Server kann 5.000 parallele Calls bearbeiten, ein PSTN Gateway mit maximal drei S2M-Schnittstellen 90 ein- oder ausgehende Calls. Bei einer angenommenen Gesprächsdauer von 3 Minuten sind dies 90 Calls in 180 Sekunden oder 0,5 Call / Sekunde. Weiter nehmen wir an, TK-Server und Gateways können als N+1 Redundanz in einem Mehrfach-Verbund betrieben werden. Sei N die Anzahl parallel auftretender Calls, P die Anzahl ein- und ausgehender Gateway-Calls je Sekunde, K die Redundanz. Dann gilt (siehe Tabelle):

3 TK-Server, 4 PSTN-Gateways:	
N = 15.000 => K = 0	keine Redundanz; jeder TK-Server ist ein SPoF
P = 2 / Sek. => K = 0	keine Redundanz; jedes Gateway ist ein SPoF
4 TK-Server, 5 PSTN-Gateways (wie in Abbildung 1.4 dargestellt):	
N = 15.000 => K = 5.000	3+1 Redundanz; der Ausfall eines TK-Servers wird verlustfrei aufgefangen
P = 2 / Sek. => K = 0,5	4+1 Redundanz; der Ausfall eines Gateways wird verlustfrei aufgefangen
5 TK-Server, 6 PSTN-Gateways:	
N = 15.000 => K = 10.000	3+2 Redundanz; der Ausfall zweier TK-Server wird verlustfrei aufgefangen, ist jedoch bei Ausfall eines TK-Server überdimensioniert und ermöglicht bei Aufteilung auf zwei TK-Server-Standorte nicht den Ausfall eines Standortes
P = 2 / Sek. => K = 1,0 / Sek.	4+2 Redundanz; der Ausfall zweier Gateways wird verlustfrei aufgefangen, ist jedoch bei Ausfall eines Gateways überdimensioniert und ermöglicht bei Aufteilung auf zwei Gateway-Standorte nicht den Ausfall eines Standortes
6 TK-Server, 8 PSTN-Gateways:	
N = 15.000 => K = 15.000	1+1 Redundanz; ermöglicht bei Aufteilung auf zwei Server-Standorte den Ausfall eines Standortes verlustfrei
P = 2 / Sek. => K = 2,0 / Sek.	1+1 Redundanz; ermöglicht bei Aufteilung auf zwei Gateway-Standorte den Ausfall eines Standortes verlustfrei

Verteilen sich die Benutzer auf zwei Standorte, die über 10 Mbit Ethernet gekoppelt sind, bietet sich folgendes Konzept an:

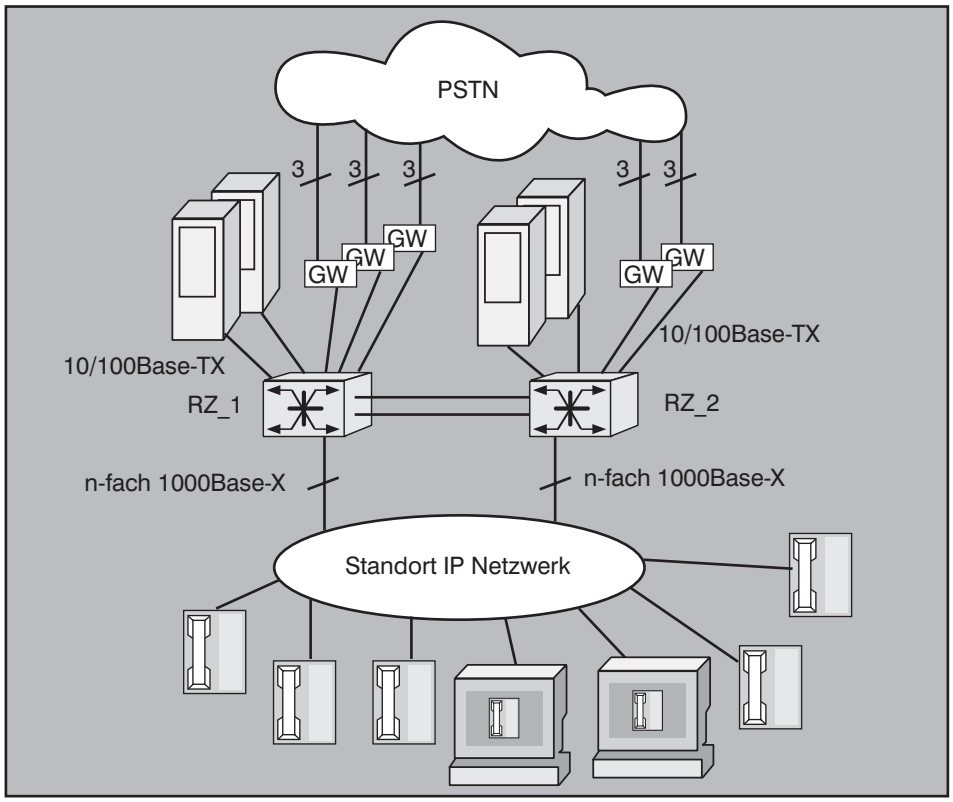


Abbildung 1.4: N+1 Redundanz von TK-Servern und Gateways an einem Standort

Die TK-Server werden auf zwei Standorte verteilt, da die gesamte Signalisierung für 10.000 Gespräche (kalkuliert werden ca. 10 Mbit für 1.000 Gespräche) die Standortkopplung überfordern würde, die Kapazität ein- und ausgehender PSTN-Gespräche (bei angenommener hälftiger Last: 4 Mbit je Standort) jedoch über die Standortkopplung abgewickelt werden kann. Als Konfiguration ergibt sich (siehe Tabelle)

6 TK-Server, 5 PSTN-Gateways (wie in Abbildung 1.5 dargestellt):	
N1 = 10.000 => K = 5.000	2+1 Redundanz; der Ausfall eines TK-Servers an Standort 1 wird verlustfrei aufgefangen
N2 = 10.000 => K = 5.000	2+1 Redundanz; der Ausfall eines TK-Servers an Standort 2 wird verlustfrei aufgefangen
P1,P2 = 1/Sek. => K = 0,5	4+1 Redundanz; der Ausfall eines Gateways wird verlustfrei aufgefangen

1.3 Redundanzverfahren

Die redundante Auslegung des Netzwerks erfordert den Einsatz von Redundanzverfahren, um auf Layer 2 Ethernet Loops zu vermeiden und um im Fehlerfall eine automatische Umschaltung auf alternative Wege zu realisieren. Da der klassische Spanning Tree eine Schaltzeit von 30 bis 90 Sekunden oder bei komplexen Konfigurationen noch länger hat (uns sind Praxismessungen bis 5 Minuten bekannt), führt er bei Telefonie zu Sessionabbruch und ist nicht zu empfehlen. Hier sollte als Layer-2 Verfahren der Rapid Reconfiguration Spanning Tree mit Schaltzeiten von unter einer Sekunde bis wenige Sekunden eingesetzt werden.

Aus denselben Gründen empfehlen wir als Layer-3 Verfahren das dynamische Routing Protokoll OSPF mit einer Schaltzeit von unter einer Sekunde bis wenige Sekunden im Gegensatz zu RIP mit Schaltzeiten im Bereich von 30 Sekunden bis mehrere Minuten. Für geroutete Verbindungen zwischen Telefon und TK-Server reicht die Aktivierung von dynamischem Routing nicht aus, sondern muss auch der Default Router Zugang redundant betrieben werden. Hierfür empfehlen wir den Einsatz des IETF Standards VRRP.

Als Konsequenz für die Netzwerk-Konfiguration ergibt sich eine redundante Anschaltung von Layer-2 Teilnetzen (z. B. ein Gebäude, mehrere Etagen, eine Etage, eine Halle oder ein Hallenteil) an zwei Layer-3 Komponenten im nächstgelegenen Netzsternpunkt (Gebäude, Gelände oder RZ). Dies können bei einer niedrigen Anzahl benötigter Schnittstellen nicht-modulare Switches sein, bei einer hohen Anzahl benötigter Schnittstellen sind wegen der höheren Systemleistung und höheren Softwarefunktionalität modulare Switches vorzuziehen. Auf verschiedene Design-Alternativen zu diesem Grundkonzept gehen wir an späterer Stelle noch detaillierter ein.

2. Netzwerk-Leistung

Zwei weitere wichtige Basiswerte für Voice-ready Netze sind die benötigte Datenrate und das maximale Delay zwischen zwei Endpunkten bzw. Teilnehmern.

2.1 Datenraten und Delay

LAN

Da im LAN üblicherweise G.711 Codierung für IP Telefonie genutzt wird, kann ein einzelnes Gespräch inklusive Signalisierung mit 100 kbit/s nach oben abgeschätzt werden (die tatsächliche Last wird im Regelfall irgendwo zwischen 84kbit/s und 96 kbit/s liegen). Bei Bildtelefonie kommt natürlich der Video-Anteil hinzu, der sich bei MPEG 1 und MPEG 2 je nach Auflösung zwischen 1 Mbit/s und 9 Mbit/s je Session bewegt. Wir beschränken uns nachfolgend auf reine Audio-Telefonie, da Bildtelefonie noch einen sehr niedrigen Verbreitungsgrad hat.

Bei 100 parallelen Gesprächen ist eine Telefonie-Datenlast von 10 Mbit/s zu kalkulieren, das entspricht 10 Prozent bei 100 Mbit Uplinks zur Endgeräte-Anbindung - von 100 Endgeräten! Ein realistischerer Wert bei Nutzung von 100 Mbit Uplinks dürfte eher bei 48 Ports oder 24 Ports, also 4,8 Prozent oder 2,4 Prozent der Uplink-Kapazität liegen, wenn auf allen Ports gleichzeitig telefoniert wird. Bei der Anbindung von 100 Endgeräten über einen 1 Gbit Uplink macht die Telefonie-Datenlast bei maximal einem Telefonat je Endgerät noch 1 Prozent aus und kann im Verhältnis zur Gesamtlast als unkritisch betrachtet werden. Wird eine Etage mit 100 Endgeräten zukünftig mit 10 Gbit Ethernet an den nächsten Netzsternpunkt angebunden, so wird die Telefonie-Datenlast nur noch 0,1 Prozent betragen.

Der kritischere Wert ist somit das Delay.

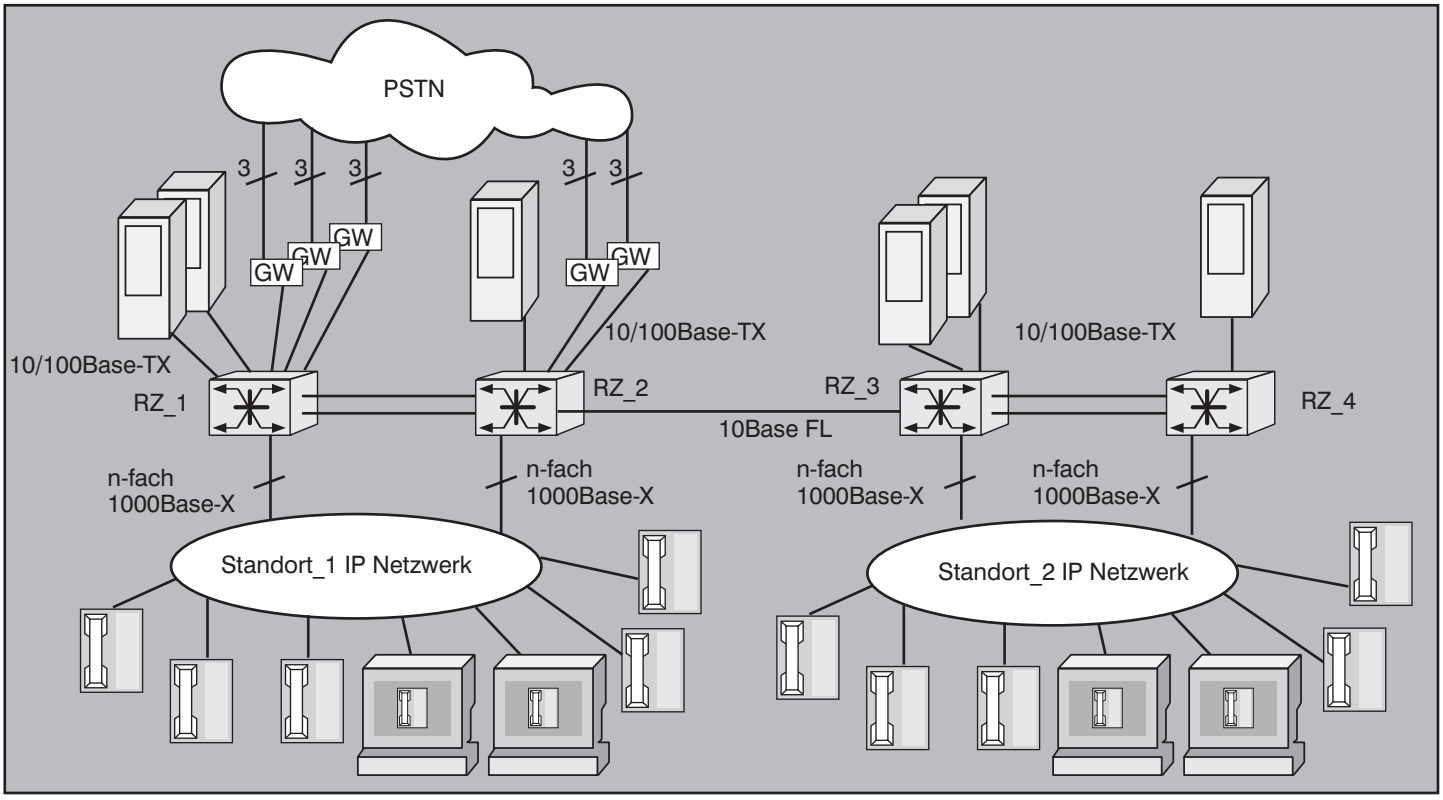


Abbildung 1.5: N+1 Redundanz von TK-Servern und Gateways bei zwei Standorten

Betrachten wir die reine Serialisierung, so ergibt sich für 1500 Byte und unterschiedliche Datenraten eine Übertragungszeit von:

10 Mbit/s:	1,2 msec
100 Mbit/s:	120 µsec
1 Gbit/s:	12 µsec
10 Gbit/s:	1,2 µsec

Aus diesem Grund raten viele Planer bei Einsatz von IP Telefonie dazu, 100 Mbit am Endgerät und 1 Gbit oder mehr als Uplink Datenrate zu fahren.

Mit entsprechenden Warteschlangen-Modellen kann ein Switch als Ein-Bediener-System modelliert und für eine Switch-Kaskade bei einer angenommenen Auslastung das Delay nach oben abgeschätzt werden (worst case Betrachtung). Für Beispielrechnungen ist die resultierende Anzahl Frames inklusive Schwankung je Auslastungswert in Abbildung 2.1 zusammengefasst. Bei einer Summenlast von 30% auf dem Uplink einer Etage (die als worst case Abschätzung schon am ersten kaskadierten Workgroup Switch der Etage anliegt) und fünf kaskadierten Switches ergibt sich ein Delay von 195 µs (siehe Abbildung 2.2 und Abbildung 2.3). Dies deckt sich mit Werten, die in der Praxis gemessen wurden. Bei einer Auslastung von 50% und 7 kaskadierten Switches ergibt sich immer noch ein Delay von 526 µs (siehe Abbildung 2.4). Voll geswitchte Netzwerke mit 100 Mbit Datenrate am Endgerät und mindestens 1 Gbit Uplink je 100 Endgeräte sind daher im Regelfall implizit „voice-ready“, d.h. für die Übertragung von IP Telefonie geeignet.

WAN

Da im WAN-Bereich immer noch Datenraten von 256 kbit/s bis 2 Mbit/s gefahren werden und 8 Mbit/s, 34 Mbit oder Metro-Ethernet vielfach nicht vorhanden sind, entsteht hier der Bedarf nach Kompression, z.B. durch Einsatz des G.729(a) Codecs, der inkl. Overhead mit Datenraten

Auslastung	durchschn. Anzahl Frames	Sigma	2 Sigma	3 Sigma	Sigma 2 (Varianz)	max. Anzahl Frames (Worst Case)
		68% der Peakzeit	95,5% der Peakzeit	99,7% der Peakzeit		
10%	0,11	0,35	0,70	1,05	0,12	**1,17**
20%	0,25	0,56	1,12	1,68	031	1,93
30%	0,43	0,78	1,56	2,35	0,61	2,78
40%	0,67	1,05	2,11	3,16	1,11	3,83
50%	**1,00**	1,41	2,83	**4,24**	2,00	**5,24**
60%	1,50	1,94	3,87	5,81	3,75	7,31
70%	2,33	2,79	5,58	8,37	7,78	**10,70**
80%	4,00	4,47	8,94	13,42	20,00	24,00
90%	9,00	9,49	18,97	28,46	90,00	99,00
95%	19,00	19,49	38,99	58,48	380,00	399,00
99%	99,00	99,50	199,00	298,50	9900,00	9999,00

Abbildung 2.1: Zusammenhang zwischen Auslastung und Anzahl Frames je Puffer / Warteschlange

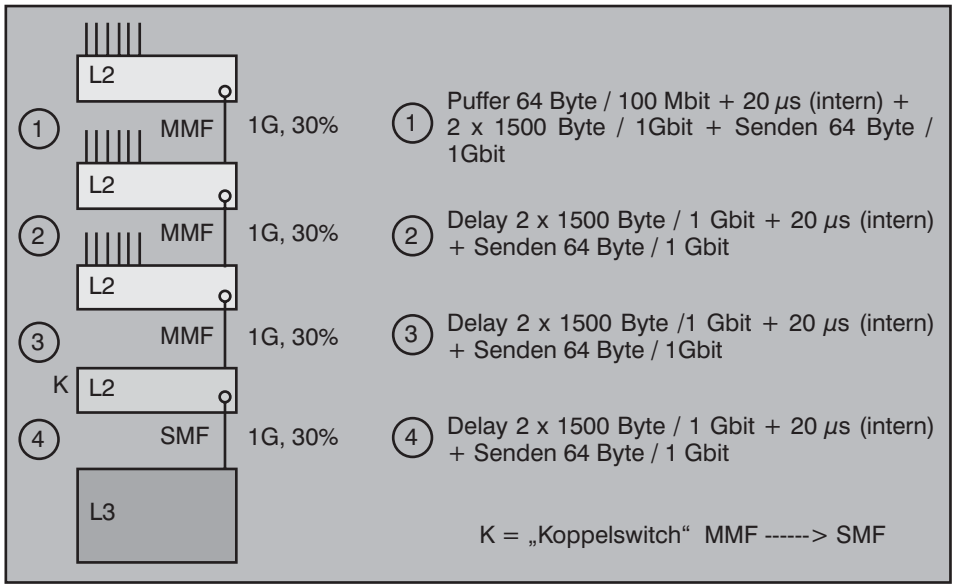


Abbildung 2.2: Einzel-Delays bei 30% Auslastung

von 24 kbit/s bis 32 kbit/s arbeitet. Proprietäre Verfahren komprimieren noch stärker, so dass bis zu 6 Gespräche über eine 64 kbit/s ISDN-Verbindung gefahren werden können (z.B. Alcatel). Je aufwändiger jedoch das Kompressionsverfahren ist, desto höher wird das Delay, so dass hier ein Trade Off entsteht und der Betreiber einen Mittelweg zwischen Datenraten und Delay suchen muss. Beachten Sie im WAN auch das Serialisierungs-Delay: Selbst wenn Sprache priorisiert wird, kann als Wartesituation die Übertragung eines einzelnen maximalen Datenframes von 1500 Byte auftreten. Bei einer Leitungskapazität von 128 kbit/s beträgt die Übertragungszeit von 1500 Byte 93,75 ms, verbraucht also schon fast das gesamte Delay Budget von 100 ms. Daher müssen 1500 Byte Datenpakete mit IP Fragmentierung verkleinert werden, um nach jedem Fragment Voice Pakete übertragen zu können: Werden Fragmente von 256 Byte erzeugt, so dauert die Serialisierung und somit maximale Wartezeit für ein Voice Paket nur 16 ms.

Auslastung von 30% an allen Uplinks					
Schritt	Empfangen von 64 Byte / 100 Mbit (µs)	Warten 3 x 1500 Byte / 1 Gbit (µs)	internes Delay (µs)	Senden von 64 Byte / 1 Gbit (µs)	Summe (µs)
1	5,12	36	20	0,512	61,632
2		36	20	0,512	56,512
3		36	20	0,512	56,512
4			20	0,512	56,512
Gesamt					195,168

Abbildung 2.3: Delay bei 30% Auslastung

Auslastung von 50% an allen Uplinks, Worst Case Failover (7 Switches)					
Schritt	Empfangen von 64 Byte / 100 Mbit (µs)	Warten 5,24 x 1500 Byte / 1 Gbit (µs)	internes Delay (µs)	Senden von 64 Byte / 1 Gbit (µs)	Summe (µs)
1	5,12	62,88	20	0,512	88,512
2		62,88	20	0,512	83,392
3		62,88	20	0,512	83,392
4		62,88	20	0,512	83,392
5		62,88	20	0,512	83,392
6		62,88	20	0,512	83,392
7			20	0,512	20,512
Gesamt					525,984

Abbildung 2.4: Delay bei 50% Auslastung

2.2 Shared LAN vs. Switched LAN

Der Trend der letzten fünf Jahre, anstelle von Shared LANs mit 100 Mbit Ethernet Hubsystemen voll geswitchte LANs mit einem einzelnen Endgerät je Switchport und full duplex Verbindungen zwischen den Switches einzusetzen, kann als Wegbereiter für die Echtzeitfähigkeit moderner Netze betrachtet werden: Das Wegfallen von Kollisionsphänomenen und Zwangspausen vor dem Senden eines Frames sowie deterministischeres Hochlastverhalten und zusätzliche Layer-2 Intelligenz für eine gegebenenfalls gewünschte Priorisierung wurden durch die Abschaffung von Hubsystemen erreicht. Jahrelang verkündeten die VoIP Hersteller, dass ein voll geswitchtes Netzwerk Design-Voraussetzung Nr. 1 bei IP Telefonie sei. Manche forderten darüber hinaus eine zusätzliche Absicherung mittels Analysemessungen. So weit, so gut.

Mit dem Boom von Wireless LAN (WLAN) und den ersten Marketing-Strategien für Voice over WLAN (VoWLAN) scheinen diese Forderungen jedoch spontanen Gedächtnisverlusten derselben Presales Leute zu unterliegen, die zuvor so vehement Realzeit-Eignung für IP Telefonie gefordert haben. Zwar wird hier der Begriff Shared LAN peinlich vermieden, WLAN ist ja auch viel moderner, doch in der Realität sind die heutigen WLAN‘s genau das: Shared LANs mit maximal 10 Mbit Datenrate bei 802.11b, was die häufigste Implementierung ist. Jeder Benutzer, der sich in derselben WLAN-Zelle bewegt, nimmt sich ein Stück von diesem 10 Mbit Kuchen. Ein einziger Druckjob einer Datei von 100 Seiten von einem performanten Laptop aus, der sich nah an der Antenne befindet, kann Ihr IP Telefonat so beeinträchtigen, dass Sie jeden Spaß daran verlieren werden. Entsprechend arbeitet die Standardisierung an einem Priorisierungsverfahren für 802.11, dessen erkennbare erste Anwendung VoWLAN ist. Einige verfügbare WLAN Telefone priorisieren sich selbst indirekt, indem sie die Wartezeit verkürzen, die der Standard bis zum Senden eines 802.11 Frames vorgibt. Ein pragmatischer Weg, über den man aber sicherlich geteilter Meinung sein kann.

Aus unserer Sicht wird IP Telefonie über WLAN Marktrelevanz erhalten, da der Mehrwert „Mobilität“ die heute noch vorhandenen Qualitätseinbußen ausgleicht, genau wie beim klassischen Mobiltelefon ja auch. Zudem wird sich auch die Wireless Technologie entweder zu höheren Datenraten plus Priorisierung oder mittelfristig zu „geswitchtem WLAN“ weiterentwickeln und möglicherweise in kombinierten Workgroup Switches niederschlagen, die einerseits eine Reihe Twisted Pair Ports und andererseits eine Reihe WLAN-Kanäle haben, die sie dediziert einzelnen Endsystemen bei der Anmeldung zuordnen. In diesem Zusammenhang ist zukünftig eine Wettbewerbs-Situation zwischen DECT und VoWLAN möglich, wobei letzteres aufgrund der Integrationsfähigkeit in IP-Netze langfristig gute Chancen hat – auch wenn der DECT Markt aktuell davon gar nichts hören will.

2.3 Lastverteilung

Bei der Implementierung von Redundanzen entsteht – zumindest auf der Ebene der Finanzierer – stets der Wunsch danach, das vorgehaltene und bezahlte Equipment auch im Normalfall zu nutzen. Dieser Wunsch führt direkt zum Thema Lastverteilung. Soweit Sie innerhalb von Layer-2 Teilnetzen bei singulären Verbindungen Link Aggregierung einsetzen oder bei Layer-3 Verbindungen OSPF ECMP nutzen, mag hier eine Effizienzsteigerung bei nur geringfügig erhöhten Betriebsaufwänden entstehen. Lastverteilung mit MSTP oder VRRP führt jedoch zu einer deutlich aufwändigeren Konfiguration und entsprechend auch komplizierteren Störfall-Analyse bis hin zur Unübersichtlichkeit. Daher empfiehlt UBN dies nicht als Lösung erster Wahl. Falls zur Leistungssteigerung solche Verfahren eingesetzt werden, sollte dies ausschließlich in einem eng begrenzten Umfang sowie in möglichst partitionierten Konfigura-

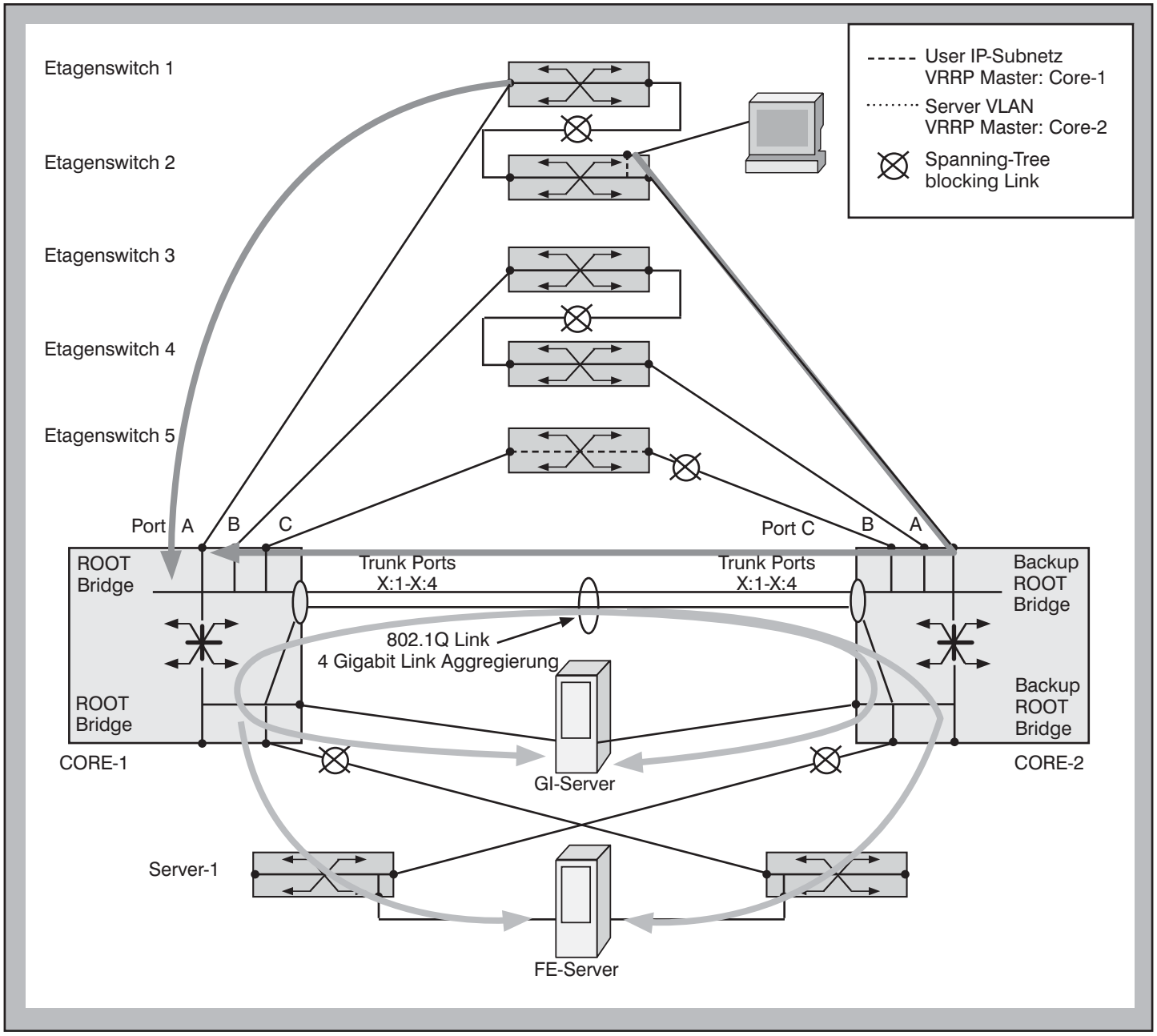


Abbildung 2.5: Lastverteilte Konfiguration bei Kombination von VRRP, STP und Link Aggregierung

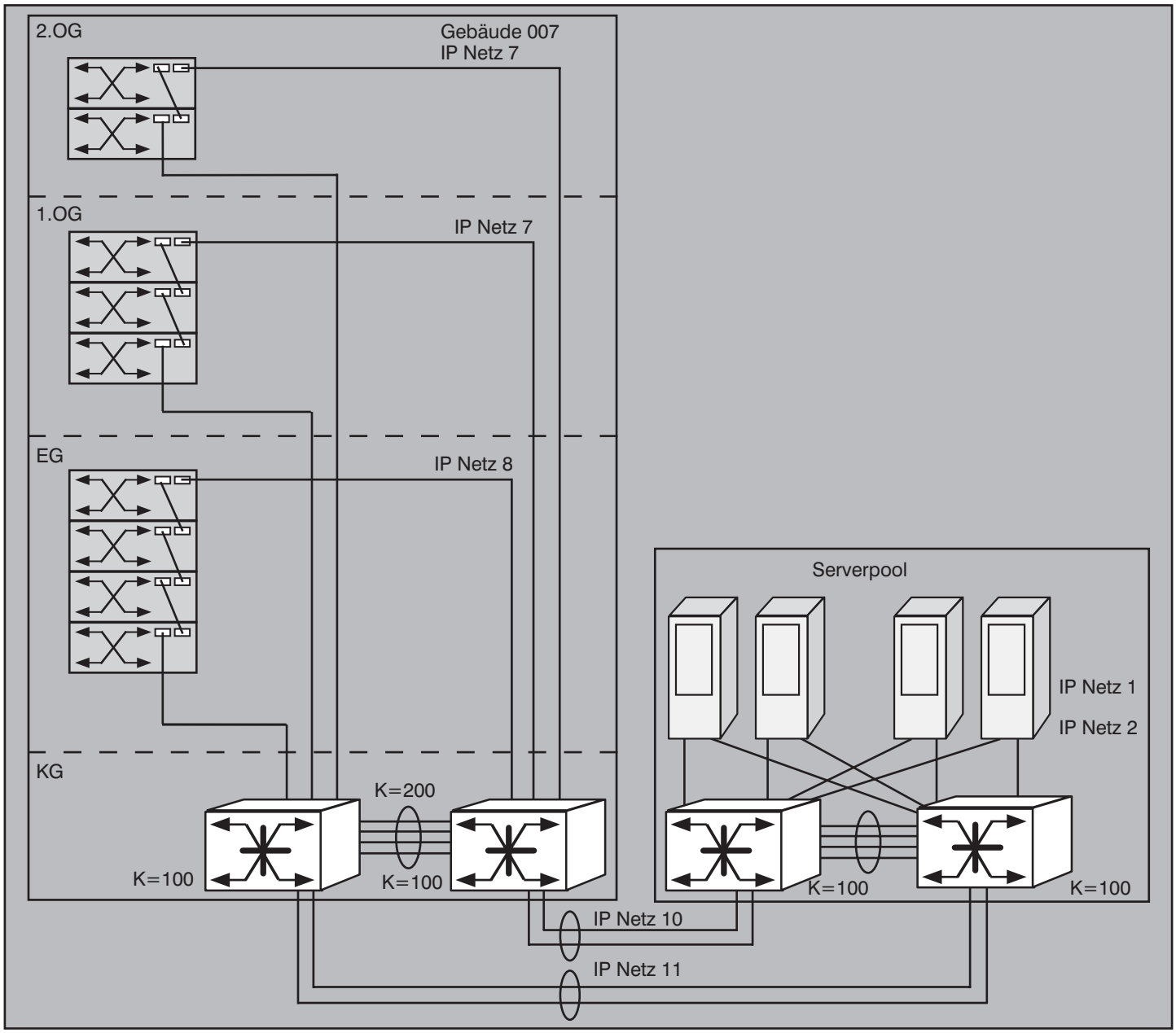


Abbildung 2.6: Lastverteilte Konfiguration bei Kombination von Link Aggregierung und OSPF Routing (1)

tionen (überschneidungsfreie MSTP‘s und VRRP-Lastverteilung über separate IP-Netze und separate physikalische Interfaces). In Abbildung 2.5 zeigen wir ein Negativ-Beispiel, in dem Spanning Tree und VRRP lastverteilt kombiniert werden. Die Lastverteilung funktioniert zwar von der Etage ausgehend über verschiedene Uplinks, da jedoch innerhalb desselben IP Subnetzes genau ein Default Router aktiv ist, verläuft die Hälfte des Etagenverkehrs über die Link Aggregierung zwischen den beiden zentralen Layer-3 Switches. Ebenso verhält es sich bei den angebundenen Servern. Auch in den Beispielszenarios aus Abbildung 2.6 und Abbildung 2.7, die auf den ersten Blick sehr übersichtlich erscheinen, funktioniert Lastverteilung über die LAG‘s nur, wenn der Switch statistische Lastverteilung oder Verteilung nach verschiedenen IP Adressen bzw. TCP/UDP Portnummern leisten kann: Da hier eine geroutete Verbindung vorliegt, trägt der Layer-3 Switch in alle Pakete seine MAC-Adresse ein – und das ist die singuläre MAC-Adresse der Link Aggregierung!

3. TK-Komponenten

TK-Komponenten lassen sich grob in drei Gruppen einteilen: TK-Endgeräte, TK-Server / TK-Anlage und Gateways. Beim Einsatz von Zusatzanwendungen wie UM, CC, CTI kommen weitere TK-Anwendungsserver hinzu.

3.1 Hardphones

Vielfach werden aktuell für IP Telefonie-Lösungen, so wie bei klassischen TK-Lösungen üblich, Handapparate installiert, die lediglich anstelle eines digitalen einen Ethernet Anschluss besitzen. Gründe hierfür liegen einerseits in dem für die Benutzer gewohnten Umgang mit einem separaten Telefon, vielleicht sogar mit der selben Bedienoberfläche wie dasjenige, welches sie vorher hatten, wenn die IP Lösung vom selben Hersteller ist; andererseits herrscht gegenüber dem PC als

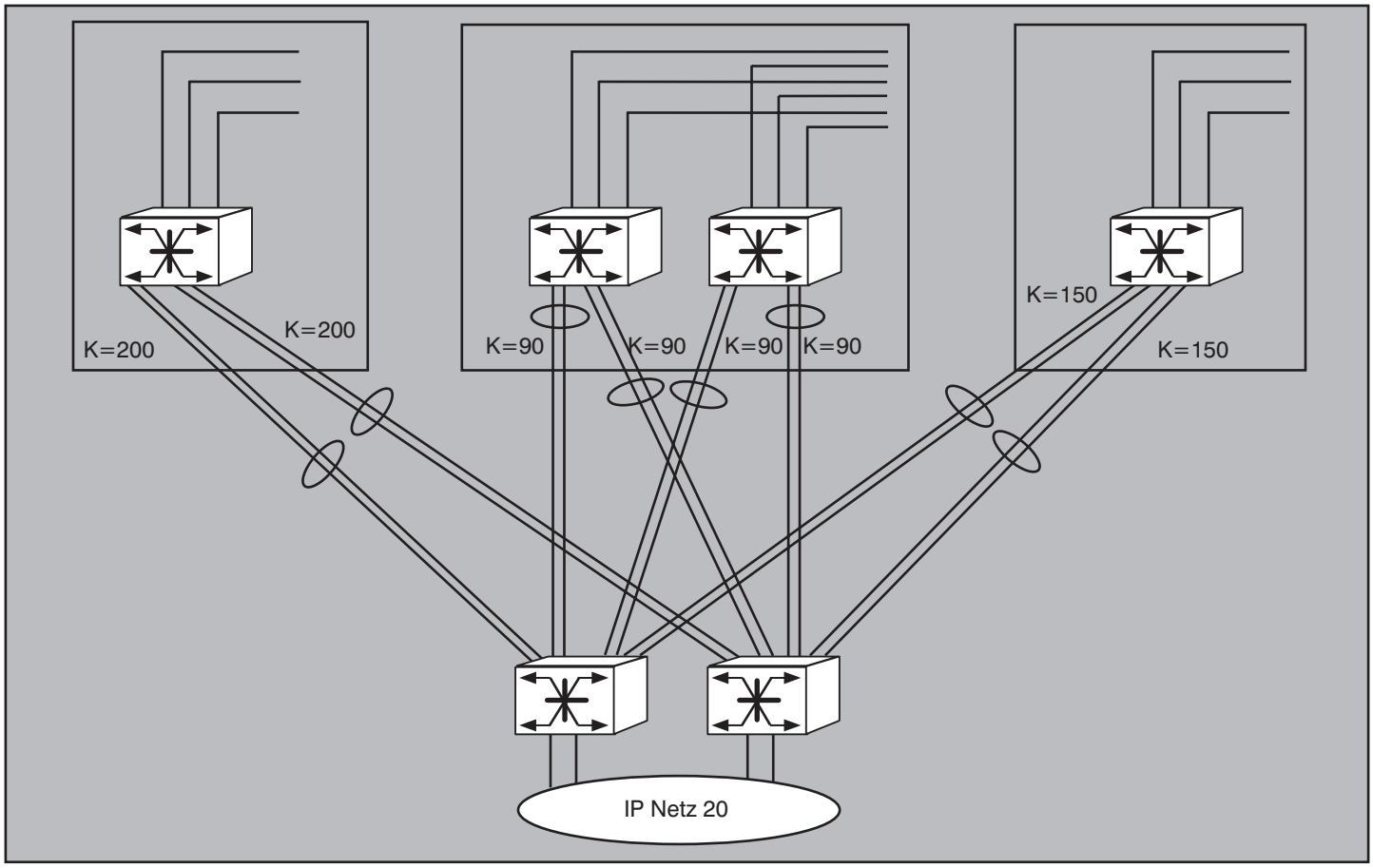


Abbildung 2.7: Lastverteilte Konfiguration bei Kombination von Link Aggregierung und OSPF Routing (2)

einziges Arbeitsgerät für IT und TK noch immer Misstrauen. Unserer Einschätzung nach ist dies eine Übergangsphase von mehreren Jahren, bis sich der PC mit Handset oder aber das Bildschirmtelefon mit Office-Oberfläche als integriertes Einzelgerät am Arbeitsplatz durchsetzt. Diese Entwicklung wird Hand in Hand gehen mit der Weiterentwicklung von DSP Chips auf Intel Motherboards und der Weiterentwicklung von Microsofts Multimedia-Kommunikation unter Windows und SIP.

Der heutige Einsatz separater Telefone hat jedoch Konsequenzen für das Design eines telefonie-geeigneten Netzwerks: Soll jedes Telefon einen eigenen LAN-Anschluss erhalten, so muss für die Implementierung eine erhebliche Mehranzahl von Anschlüssen vorgesehen werden. Als Kosten sparende Alternative sind Telefone mit integriertem Ethernet Miniswitch einsetzbar, bei denen der PC mit dem Telefon kaskadiert wird, um im Büro Datensteckdosen und im Verteilerraum Switchports einzusparen, wie in Abbildung 3.1 gezeigt. Allerdings sind Telefone mit integriertem Miniswitch etwas teurer als Telefone mit einem einzelnen Ethernet Port. Wobei letztere oft die so genannten „Entry“ Modelle aus den Hersteller-Produktlinien sind, die sowieso mit reduzierter Oberfläche und Funktionalität vermarktet werden (weniger Funktionstasten, teilweise keine Frei-

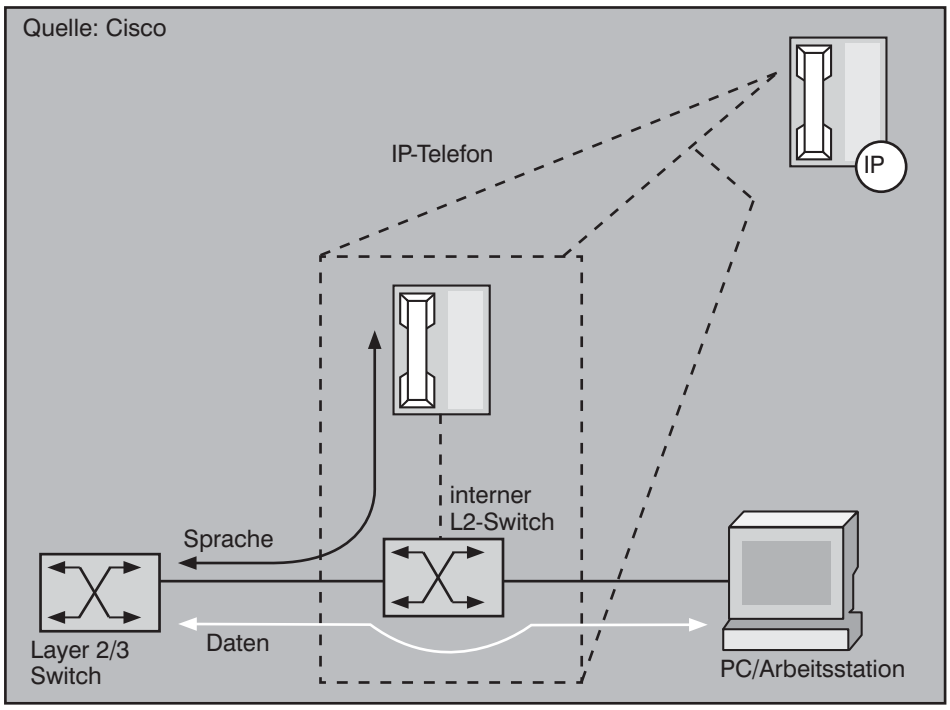


Abbildung 3.1: Ethernet Telefon mit eingebautem Mini-Switch

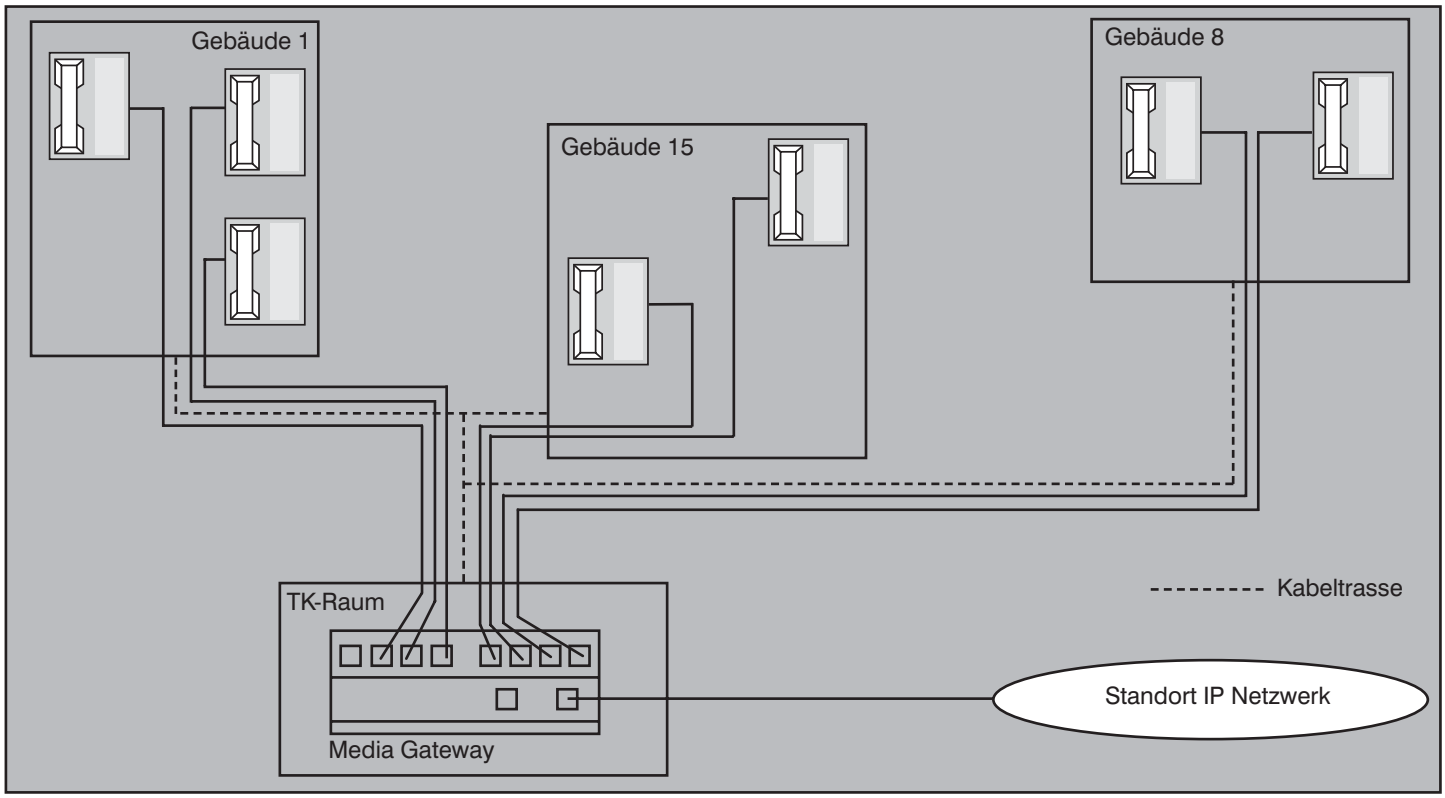


Abbildung 3.2: Anbindung analoger Endgeräte über ein Media-Gateway

sprecheinrichtung, keine Schnittstellen für Headset o.ä.). Bei Neubauprojekten kann mit der kaskadierten Lösung eine Einsparung der benötigten Portzahl von 30 bis 40 Prozent erreicht werden (z.B. nur noch zwei statt drei Anschlüsse je Arbeitsplatz). Um klassische Telefonie vollfunktional abzubilden, müssen IP Telefone von einem zentralen Punkt aus mit Strom versorgbar sein, schon aus dem Grund, dass Telefonieren auch nach einem Ausfall des Raumstromkreises noch möglich sein soll. In diesem Fall ist der IEEE Standard 802.3af anwendbar (PoL, Power over LAN oder auch PoE, Power over Ethernet), soweit die Geräte über Kupferverbindungen mit Twisted Pair angeschlossen sind. Der 802.3af Standard wurde jedoch nicht nur für Telefone definiert sondern allgemein für Endgeräte mit niedriger Leistungsaufnahme wie WLAN Access Points, Kameras oder andere Gebäudeinfrastruktur-Komponenten. Auf die technische Realisierung gehen wir beim Punkt „Netzkomponenten“ etwas näher ein. Soll keine zentrale Stromversorgung genutzt werden, so verfügen alle Ethernet Telefone auch über einen separaten Stromanschluss (mit Trafo-Anpassung von 48V auf 220V), der sich teilweise für eine Unter-Tisch-Montage eignet, was zur Minimierung von Störfällen (Stöße, die den Steckkontakt lösen oder lockern, o.ä.) hilfreich ist. Natürlich sind auch Mischkonzepte denkbar, bei denen lediglich „wichtige“ Telefone zentral mit Strom versorgt werden. Aus Gründen der Einheitlichkeit, insbesondere für Betriebs- und Umzugsrichtlinien, sind solche Lösungen weniger empfehlenswert.

3.2 Softphones

Sollen Softphones zum Einsatz kommen, so müssen die ggf. notwendigen PC-Auf-

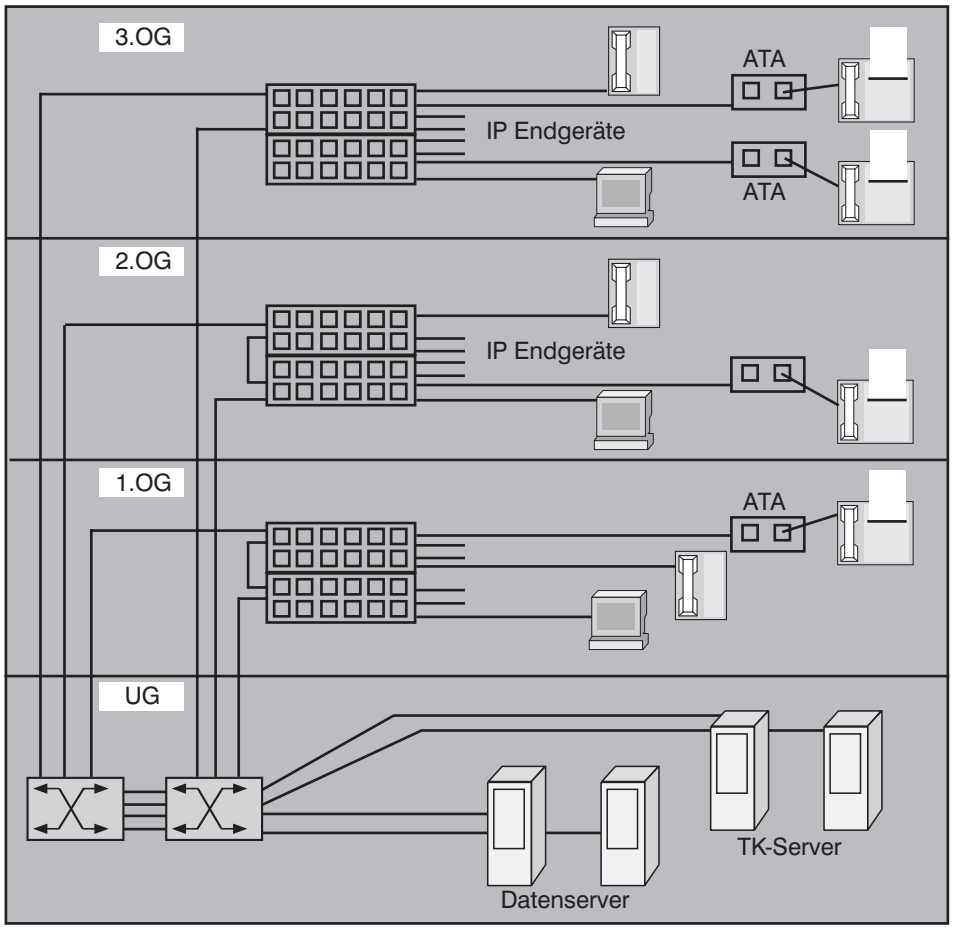


Abbildung 3.3: Anbindung analoger Endgeräte über einen Analog-Adapter

rüstungen wie USB-Schnittstelle, Headset, Handset, Soundkarte geplant werden. Wir raten hier dringend dazu, so wie es auch für NIC‘s gute Praxis ist, für alle TK-Zusatzkomponenten in PC‘s oder Laptops Unternehmens-Standards festzuschreiben, da jede dieser Komponenten eigenes Betriebs-Know How erfordert und da diese Komponenten viel zur guten oder schlechten Qualität einer Lösung beitragen, was insbesondere für die Soundkarte gilt, aber auch Headset und Handset sollten vom Hersteller der jeweiligen TK-Lösung technisch unterstützt oder sogar explizit empfohlen werden.

Sollen Softphones zum Einsatz kommen, so muss bei der Produkt-Evaluierung untersucht werden, wie gut das Softphone die klassischen Telefonfunktionen bzw. Leistungsmerkmale abbildet und ob die Benutzeroberfläche inklusive Konfiguration der Benutzer setzbaren Parameter (Rufumleitung, Adressbücher, teilweise Benutzerprofil, tageszeitabhängige Schaltungen etc.) intuitiv bedienbar ist. Einige Softphone-Lösungen haben noch nicht den vollen TK-Umfang der klassischen Handapparate und / oder unterstützen noch nicht die herstellereigene Signalisierung (z.B. bei Cisco).

Das Problem der erhöhten Anschlusszahl für Telefone hat sich mit dem Einsatz von Softphones erledigt, da für den PC in jedem Fall ein Anschluss vorzusehen ist.

3.3 Mobile Endgeräte

IP-fähige mobile Endgeräte sind im wesentlichen WLAN Telefone, PDAs mit WLAN Anschluss und Laptops. Letztere fallen unter die Kategorie Softphone, wobei gegebenenfalls technisch ein WLAN-Anschluss anstelle eines Ethernet Anschlusses genutzt wird. WLAN Telefone, PDA‘s und Laptops mit WLAN Anschluss unterliegen den Designüberlegungen für Wireless LANs, insbesondere hinsichtlich Datenrate und Datenschutz. Sollen verstärkt WLAN Telefone oder PDA‘s zum Einsatz kommen, so muss möglicherweise eine flächendeckende WLAN Infrastruktur in die Planung einbezogen werden. In einigen Fällen wird sich der WLAN Bedarf auf besondere Bereiche wie Besucherzonen, VIP-Lounges, Besprechungsräume, schwer verkabelbare Produktionshallen o.ä. beschränken.
DECT Telefone werden im Regelfall über Basis-Stationen mit klassischen digitalen Interfaces eingebunden, GSM Telefone werden mittels physikalischer Gateway-Schnittstellen zum PSTN / Mobilfunknetz und Mobility-Software eingebunden, die für das Mobiltelefon einige Leistungsmerkmale der TK-Lösung verfügbar macht und dem Mobiltelefon ermöglicht, wie eine Nebenstelle der Anlage behandelt zu werden.

3.4 Analoge Endgeräte

Bei den meisten IP Telefonie-Lösungen muss die Anbindung verbleibender analoger Endgeräte vorgesehen werden, seien es Faxe, Modems oder andere Büro-Infrastruktur-Komponenten. Obwohl seit vielen Jahren gut funktionierenden Faxserver-Lösungen verfügbar sind, haben diese es bis dato nicht vermocht, die klassischen Faxgeräte zu verdrängen. Handelt es sich um ein Gebäude oder Gelände, in dem bereits klassische Telefonverkabelung zu allen Anschlüssen liegt, können Faxgeräte weiter wie bisher sternförmig an den Sternpunkt angeschaltet werden, an dem zuvor die TK-Anlage stand. Hier können alle Analoganschlüsse je nach gewähltem Hersteller mittels Konzentrator, Analog-Gateway, Media-Gateway oder Gateway-Einschub in einen Router, Stackable Switch etc. angebunden werden (siehe Abbildung 3.2).

Handelt es sich um ein Neubau-Projekt, in dem keine separate Zweidraht- oder Twisted Pair Telefonverkabelung verlegt werden soll, so müssen analoge Endgeräte vor Ort mittels IP-Adapter (ATA, Analoger Terminal Adapter) an das Ethernet Netz angeschlossen werden (siehe Abbildung 3.3). Die hierfür angebotenen Komponenten verfügen im Regelfall über einen oder zwei analoge Ports und eine 10/100Base-TX Ethernet-Schnittstelle. Sie transformieren den analogen Datenstrom in Ethernet/IP Pakete. Bei einer starken Streuung analoger Anschlüsse müssen entsprechend viele Analog-Adapter sowie die zugehörigen Wandanschlüsse und Switchports im Verteilerraum berücksichtigt werden. Gibt es stattdessen Büro-Inseln, an denen die Analoganschlüsse konzentriert werden können (Sekretariate), so kann an diesen Konzentrationspunkten möglicherweise Kosten sparend ein Analog-Gateway mit entsprechender Portkonzentration eingesetzt werden.

3.5 TK-Server / TK-Anlage

Die zentrale Steuerkomponente einer TK-Lösung kann als Standardserver mit TK-Software oder als Hardwaresystem mit IP-

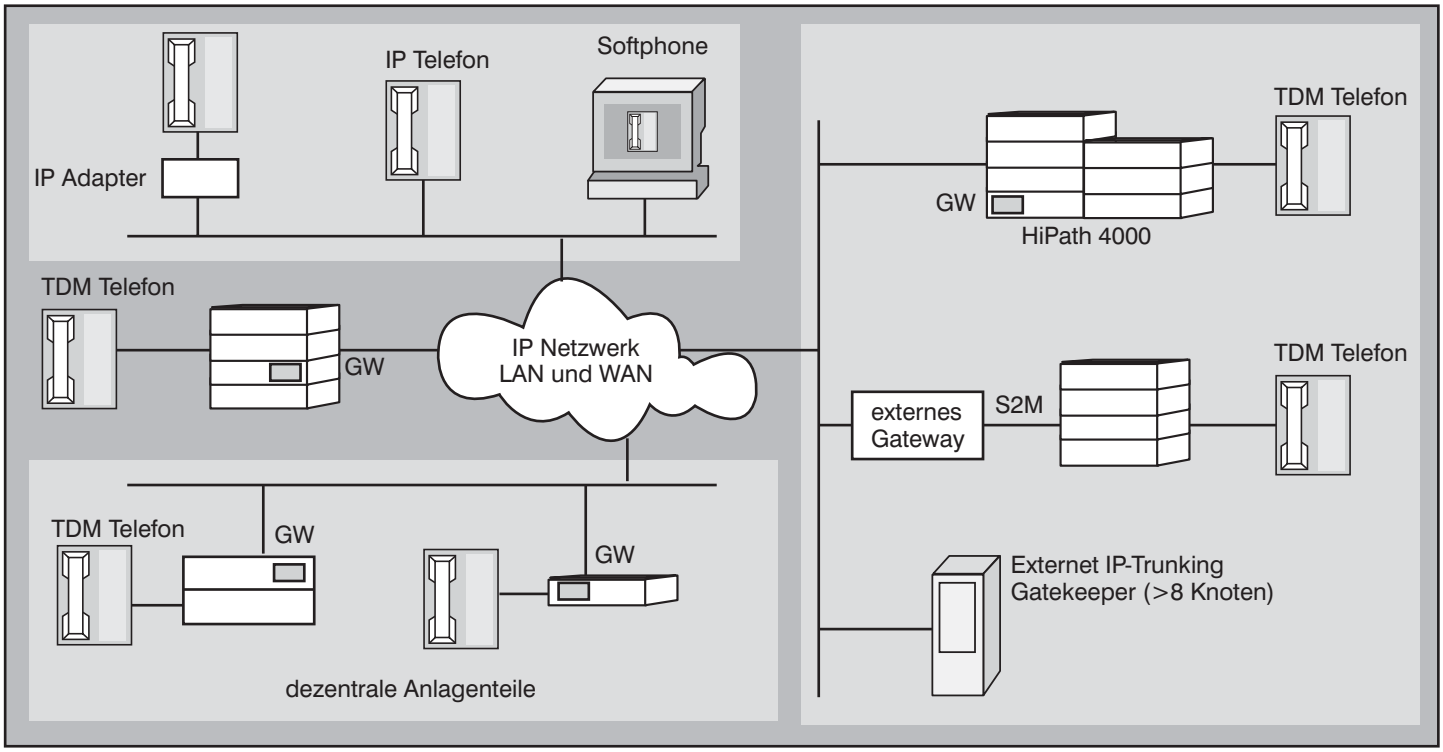


Abbildung 3.4: IP-fähige TK-Anlage mit Gateway-Einschubtechnik

Einschüben realisiert sein. Wir unterteilen die heute auf dem Markt verfügbaren Architekturen in drei Kategorien:

- IP-fähige TK-Anlage (Gateway-Prinzip)
- Verteilte Architektur
- IP Softswitch

IP-fähige TK-Anlage

Die IP-fähige TK-Anlage ähnelt noch am meisten der klassischen Lösung. Die zentrale Intelligenz ist ein Chassis- oder Shelf-System mit proprietärem Betriebssystem. Das Chassis zusätzlich zu den klassischen Einschüben (analog, digital, DECT-Basisstation, S0- oder S2M-Trunk, ...) IP-Einschübe erhalten, die als Gateway zwischen IP-Telefonie und der anlageninternen TDM-Technik arbeiten (z.B. Siemens HiPath 4000, HiPath 3000, Tenovis Integral 55). Die Anzahl der je Gateway-Einschub konfigurierbaren IP-Telefone liegt zwischen 30 und 240. Jeder Gateway-Einschub benötigt einen Ethernet Switchport.

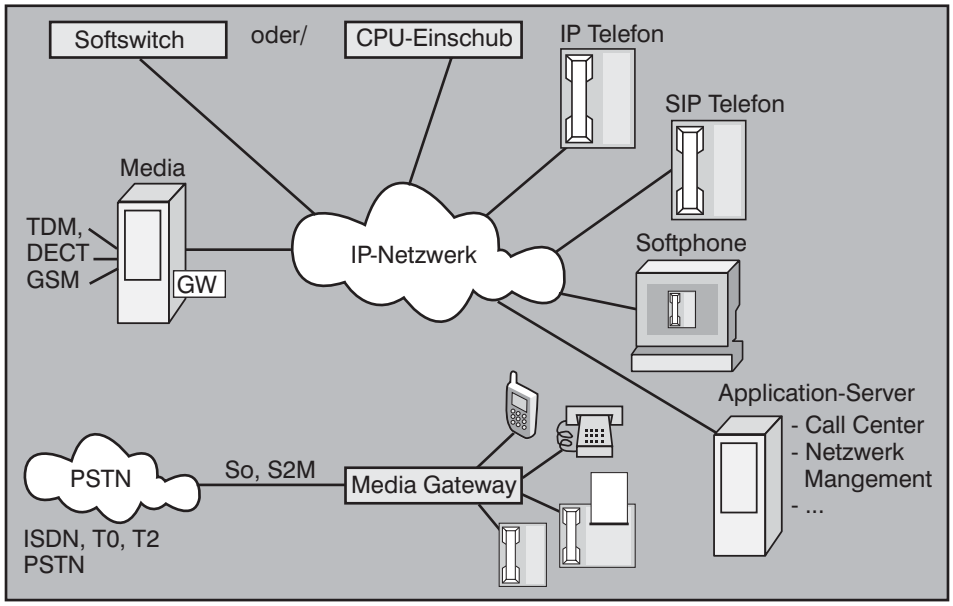


Abbildung 3.5: Dezentrale Hybrid-Architektur mit Softswitch

Bei den Gateway-Einschüben ist unbedingt ein vernünftiges Backup-Konzept zu fordern: Ohne Backup-Möglichkeit können bei Ausfall eines Gateway-Einschubs alle auf diesem Einschub definierten Benutzer nicht mehr telefonieren. Eine 1:1 Zuordnung (1 Backup Modul je aktivem Einschub) ist hier als Notlösung anzusehen, stattdessen ist eine N:1 Lösung (1 Backup Modul in derselben Anlage übernimmt dynamisch die Sessions eines ausgefallenen Gateway-Einschubs).

Teilweise unterstützen IP-fähige TK-Anlagen verteilte Konzepte, bei denen abgelagerte Anlagenteile (Shelfs, Access Points) keine sternförmige Direktanschaltung mehr erhalten müssen, sondern über das IP-Netzwerk (mit IP Trunking) dezentralisiert angebunden werden können, wie in Abbildung 3.4 gezeigt. An die Access Points können wiederum klassische und IP-Anschlüsse angeschaltet werden. Handelt es sich um ein reines IP-Konzept, ist der Einsatz von Access Points jedoch meist teurer als die Gateway-Einschübe in der zentralen Anlage.

Insgesamt ist dieser Anlagen-Architektur noch am stärksten anzumerken, dass sie der klassischen Welt verhaftet ist.

Dezentrale Hybrid-Architektur

Bei einer dezentralen Hybrid-Architektur verfügt der Hersteller über beide Elemen-

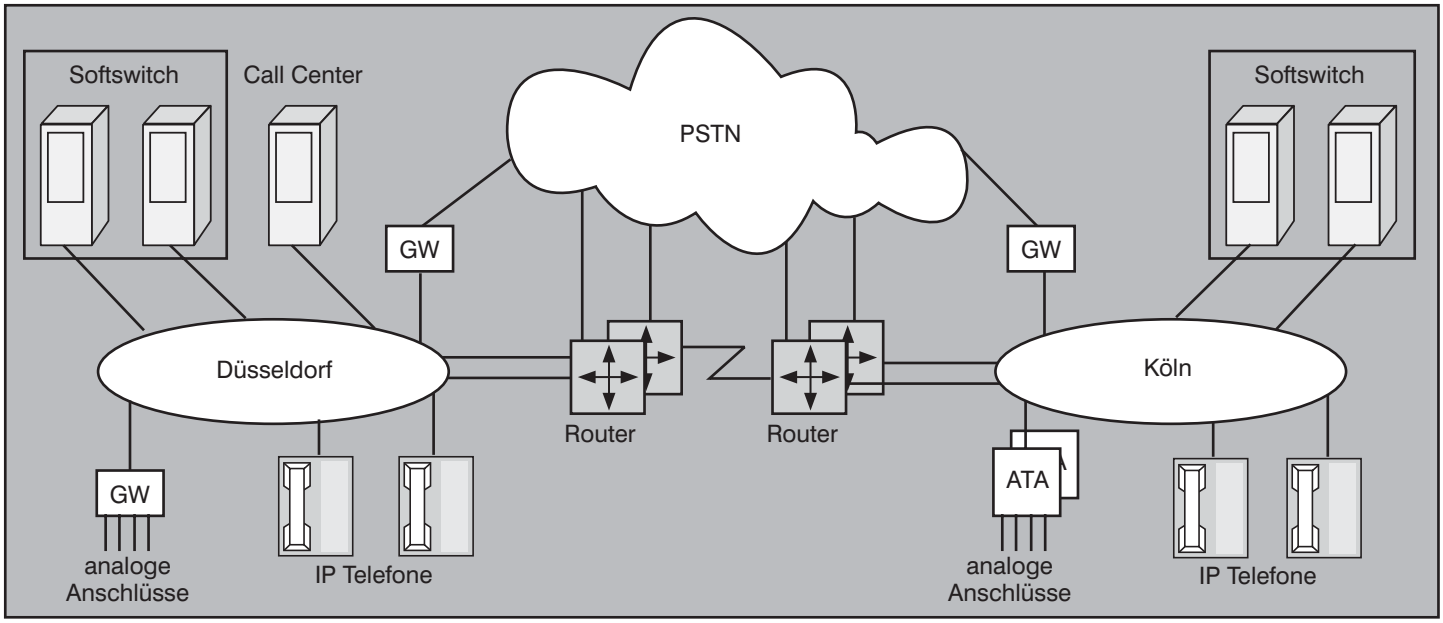


Abbildung 3.6: IP Softswitch Architektur

te: klassische TK-Anlagen und IP Softswitches als zentrale Steuerkomponente (siehe Abbildung 3.5). Die Softswitches laufen teilweise auf Standardbetriebssystemen, meistens Linux, oder einem Realzeitsystem (z.B. VxWorks) Die klassischen Komponenten können weiterhin als Media-Gateways genutzt, aber dezentral über IP angeschaltet werden (ähnlich wie bei den IP-fähigen TK-Anlagen die Access Points). Teilweise können „CPU-Einschübe“ in die Gateways eingebaut werden, die als - meistens funktional eingeschränktes - Backup arbeiten, wenn der Softswitch oder die Verbindung dorthin ausgefallen ist. Diese Einschübe werden unter Remote Survivability, Local Survivability Processor (LSP), oder ähnlich phantasievollen Namen vermarktet.

Bei Alcatel, Avaya und Nortel sind sowohl moderne kleine Chassis als auch die Flagschiffe der klassischen TK (OmniPCX 4400, Definity, Meridian) als Media Gateway durch den Softswitch steuerbar. Mit diesen Media-Gateways können alle Anschlüsse der klassischen Welt (analog, digital, DECT, PSTN, ...) realisiert werden, die noch nicht migriert sind oder dauerhaft weiter genutzt werden müssen.

Hat ein Anwender eine reine IP-Welt, so benötigt er lediglich IP-Telefone / Softphones und den Softswitch als TK-Server (zuzüglich Backup-Server). Aber wer hat die schon? Mindestens der PSTN-Zugang muss ja als Gateway-Funktion realisiert werden – wofür bei den verteilten Architekturen typischerweise ein Media-Gateway mit PSTN Trunk-Modul zum Einsatz kommt.

Da bei dezentralen Hybrid-Architekturen mit Softswitches einerseits je nach Bedarf völlig flexibel IP und non-IP Endgeräte gemischt und migriert werden können, andererseits über den Softswitch zukünftige Erweiterungen und Erhöhung der maximalen Anschlusszahlen leicht implementierbar sind, halten wir diese Architektur für diejenige, die Migrationsbedarfe und Zukunftssicherheit am besten abdeckt.

IP Softswitch

Die dritte Lösungsgruppe wurde zusammen mit der IP Telefonie geboren, hat ganz klar die IP-Technologie im Fokus und basiert rein auf einem IP Softswitch als zentrale Steuerkomponente, im Regelfall auf der Basis von Standardservern und Windows oder Linux Betriebssystem (siehe Abbildung 3.6). Als bekanntester Ver-

treter dieser Architektur ist Cisco zu benennen. Media Gateways oder Terminal Adapter sind am ehesten zur Anbindung analoger, seltener für digitale Anschlüsse verfügbar, DECT Integration wird nicht mehr von Cisco entwickelt sondern stattdessen auf WLAN IP Telefonie gesetzt. Bei der Cisco-Lösung ist zu vermerken, dass die Gateway-Funktion und auch die Remote Backup Funktion (SRST, Survivable Remote Site Telephony) auf die Router ausgelagert wird. Andere Hersteller reiner Softswitch-Lösungen verwenden eher standalone Gateways für analoge Anschlüsse und den PSTN-Zugang.

Die reine Softswitch-Architektur hat die wenigsten „Altlasten“ und ist oft am besten in die IP-Welt integrierbar oder insgesamt an neue Dienste anpassbar (z.B. SIP, Video, Web-Integration, Collaboration, Programmierschnittstellen wie XML, TAPI, JTAPI, JSAPI). Demgegenüber fehlt vielfach der direkte Bezug zur klassischen Welt und somit zu optimierten Migrationspfaden von Anwendern mit einer hohen Anzahl klassischer TK-Anschlüsse.

3.6 PSTN-Gateways

Eine IP Telefonie-Lösung ohne PSTN-Zugang ist heute nicht einsetzbar, da die große Mehrheit aller Telefone nach wie vor nur über das PSTN-Netz erreichbar ist. Alle guten Lösungen müssen daher über PSTN-Gateways verfügen. Je nach Kapazitätsbedarf ist der parallele Betrieb mehrerer S2M-Schnittstellen in einem oder mehreren Gateways erforderlich. Dies sind je nach Anlagen-Architektur standalone-Komponenten oder Einschübe in größere oder kleinere Media-Gateways, Layer-2/3 Switches oder Router. Auch Standard-PC‘s mit ISDN Karten und Gateway-Software können zum Einsatz kommen. Da die Enterprise-Lösungen für IP Telefonie mit proprietärer Signalisierung arbeiten, muss das Gateway die Signalisierung der jeweiligen Herstellerlösung unterstützen – folglich kommt im Regelfall nur ein Produkt dieses Herstellers infrage. Für den Fall, dass das standortübergreifende IP-Netzwerk nicht verfügbar ist oder nicht genügend Bandbreite zur Verfügung stellen kann, sollte das PSTN-Gateway zur Umleitung der standortübergreifenden Telefonie über das PSTN-Netz nutzbar sein (PSTN-Rerouting).

Ähnlich wie bei IP Gateway-Einschüben in klassischen Anlagen ist für den PSTN-Zugang ein Backup Konzept erforderlich. Am günstigsten ist hier die Einrichtung eines Gateway-Pools, der die ein- und ausgehenden PSTN-Gespräche dynamisch handhabt und mit soviel Überkapazität ausgestattet ist, dass der Ausfall eines Gateways verlustfrei verkraftet werden kann.

Ein Konzept, wo und wie viele Gateways betrieben werden, ist Bestandteil einer

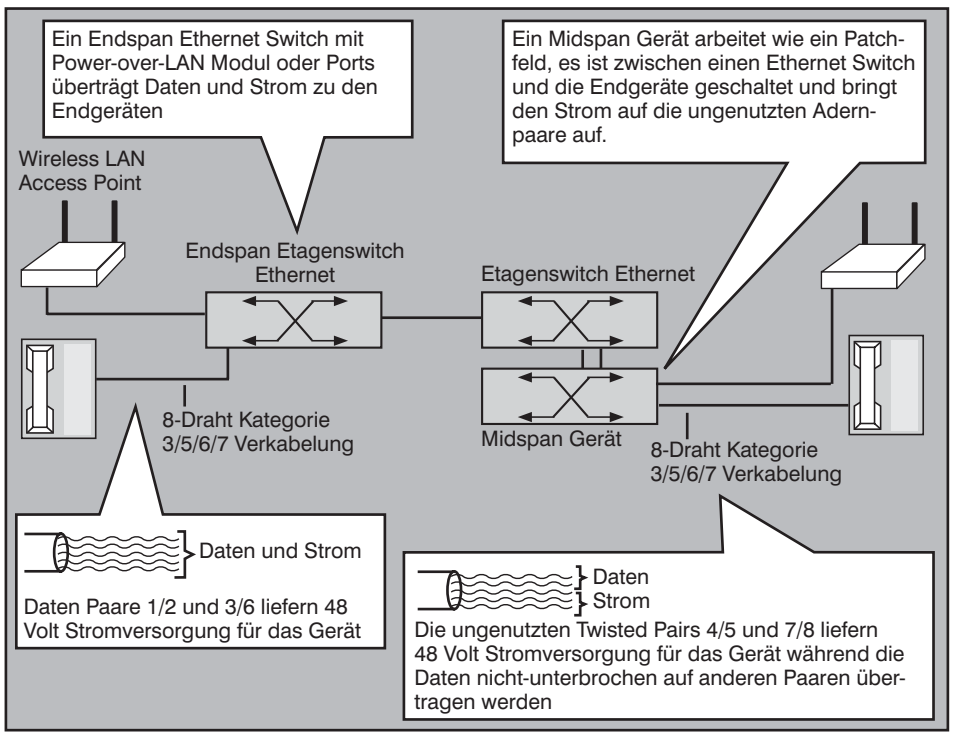


Abbildung 4.1: Zentrale Stromversorgung von Endgeräten über Kupferkabel mit Endspan und Midspan

Design-Planung. Sollen Kunden eine lokale Anwahl-Nummer nutzen, muss in dem betreffenden Kundenkontakt-Standort ein PSTN-Gateway betrieben werden; meistens ist in diesem Fall eine geringe Anzahl von PSTN-Kanälen ausreichend (4fach S0 oder 1fach S2M). Entfällt der Bedarf nach lokaler Einwahl (z.B. durch die Einrichtung von kostenfreien Service-Nummern) und ist zwischen den Standorten ausreichende WAN-Kapazität für alle externen Gespräche vorhanden, kann der Betrieb von PSTN-Gateways inklusive Backup auf einen oder wenige zentrale Standorte konzentriert werden.

4. Telefonie-geeignete Netzkomponenten

4.1 Passive Infrastruktur

Bei Migrations-Projekten oder Neuinstallationen stellt sich zuerst die Verkabelungs-Frage. Einsparungs-Potenzial durch PC-Telefon-Kaskadierung haben wir in Punkt 3. aufgezeigt. Anbindung analoger und digitaler Telefone sowie beliebiger anderer Endgeräte mit Kupfer-Anschluss ist über eine dienstneutrale Twisted Pair (TP) Verkabelung möglich. Probleme treten eher bei Migrationsprojekten mit vorhandener Verkabelung auf:

- Wurde für Telefonie eine separate, weil kostengünstige Zweidraht-Verkabelung verlegt, ist diese für IP Telefonie (Ethernet) nicht nutzbar.
- Soll eine zentrale Stromversorgung über die Verkabelung erfolgen, ist LWL zum Endgerät gar nicht nutzbar, ansonsten müssen Telefone über Konverter angeschlossen werden, da Telefone mit LWL-Ports nicht verfügbar sind.
- Liegt noch eine Typ-1 Verkabelung (vier Adern), so kann lässt sich nur eine Endspan, keine Midspan Stromversorgung implementieren. Gleiches gilt bei 8-adriger Verkabelung, die jedoch an der Datendose für den Anschluss zweier Endgeräte auf 2x4 Adern gesplittet ist.
- Liegt Typ-1 Verkabelung mit Kurschlussbrücken in den Dosen (für Token Ring), so müssen entweder die Brücken entfernt werden oder der Anschluss muss im half-duplex Modus gefahren werden. Dies bedeutet teilweise eine Festkonfigurierung der Switchports, da half-duplex bei Autonegotiation Probleme bereiten kann.

Für die zentrale Stromversorgung von Telefonen definiert der IEEE 802.3af Standard zwei mögliche Alternativen (siehe Abbildung 4.1):

- Endspan, d.h. Stromversorgung vom Switch aus, in diesem Fall über die zur Datenübertragung genutzten Adern
- Midspan, d.h. Stromversorgung von einer zwischen Switch und Endgerät angeschalteten Stromversorgungs-Komponente, als Power Hub oder Power Patch Panel bezeichnet; in diesem Fall über die nicht zur Datenübertragung genutzten Adern.

Für weitergehende Informationen zu Power over LAN verweisen wir auf den Insider Beitrag von Markus Schaub vom September 2001. Midspan Stromversorgung ist wie zuvor erwähnt bei Vierdraht-Verkabelung nicht nutzbar, da hier alle Adern für Datenübertragung genutzt werden, die Stromeinspeisung bei Midspan jedoch auf ungenutzte Adern erfolgen muss. Folglich funktioniert Midspan auch bei Gbit Ethernet nicht, da hier alle 8 Adern für Datenübertragung genutzt werden. Allerdings sind derzeit noch keine Telefone mit Gbit Ethernet Anschluss verfügbar.

4.2 PoL Switches oder Power Hubs?

Der Einsatz von PoL Switches spart die Hälfte an Patchkabeln (was in einem Verteilerschrank mit 48 bis 144 realisierten Anschlüssen erheblich ist!), führt aber zu Mehrkosten bei den aktiven Komponenten (die aktuell jedoch deutlich sinken) sowie möglicherweise zu Abhängigkeiten zwischen Switchhersteller und Telefon. Dies ist jedoch als Übergangsphänomen zu werten, da inzwischen zunehmend neue Telefone und neue Switches ausgeliefert werden, die 802.3af standardkonform sind.

Bei Workgroup Switches sind vielfach nur

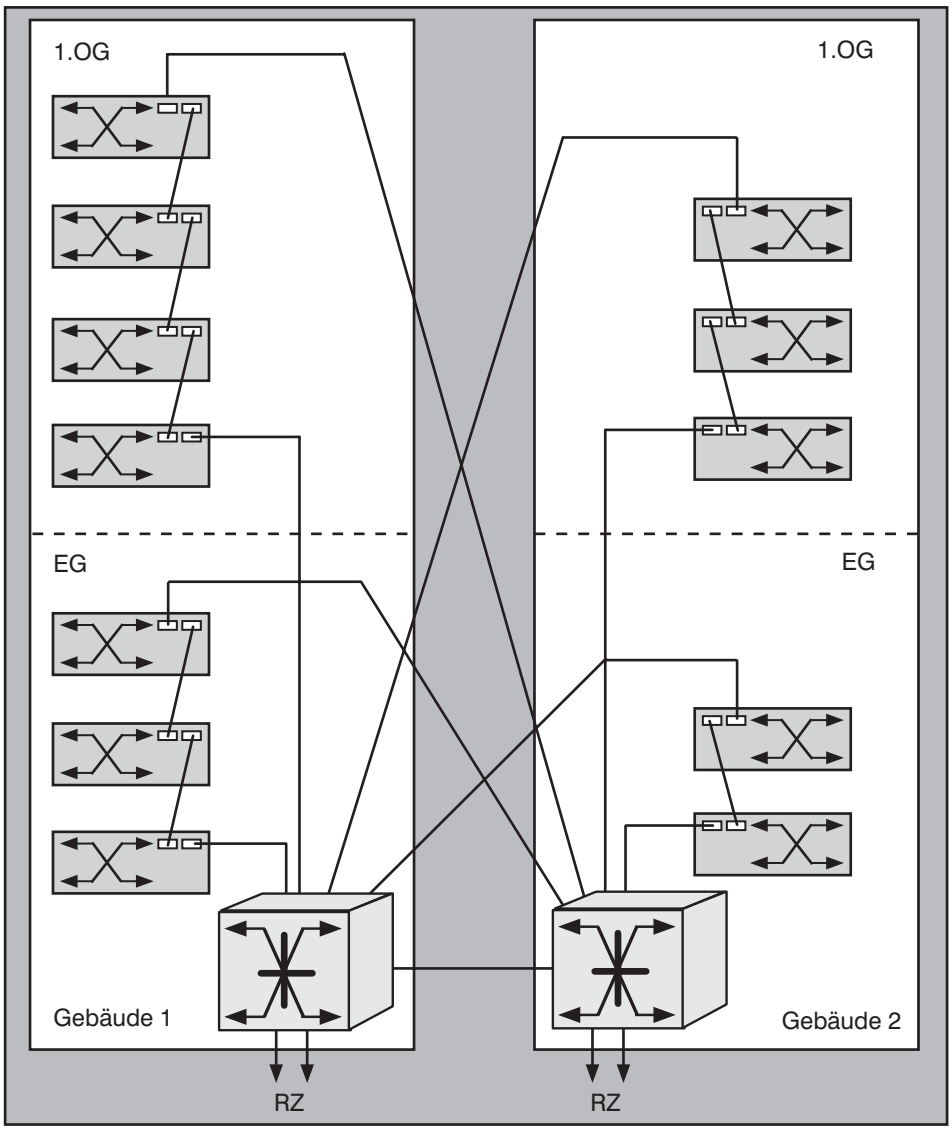


Abbildung 5.1: Redundantes Design mit maximal vierfach kaskadierten Workgroup Switches im Endgeräte-Bereich

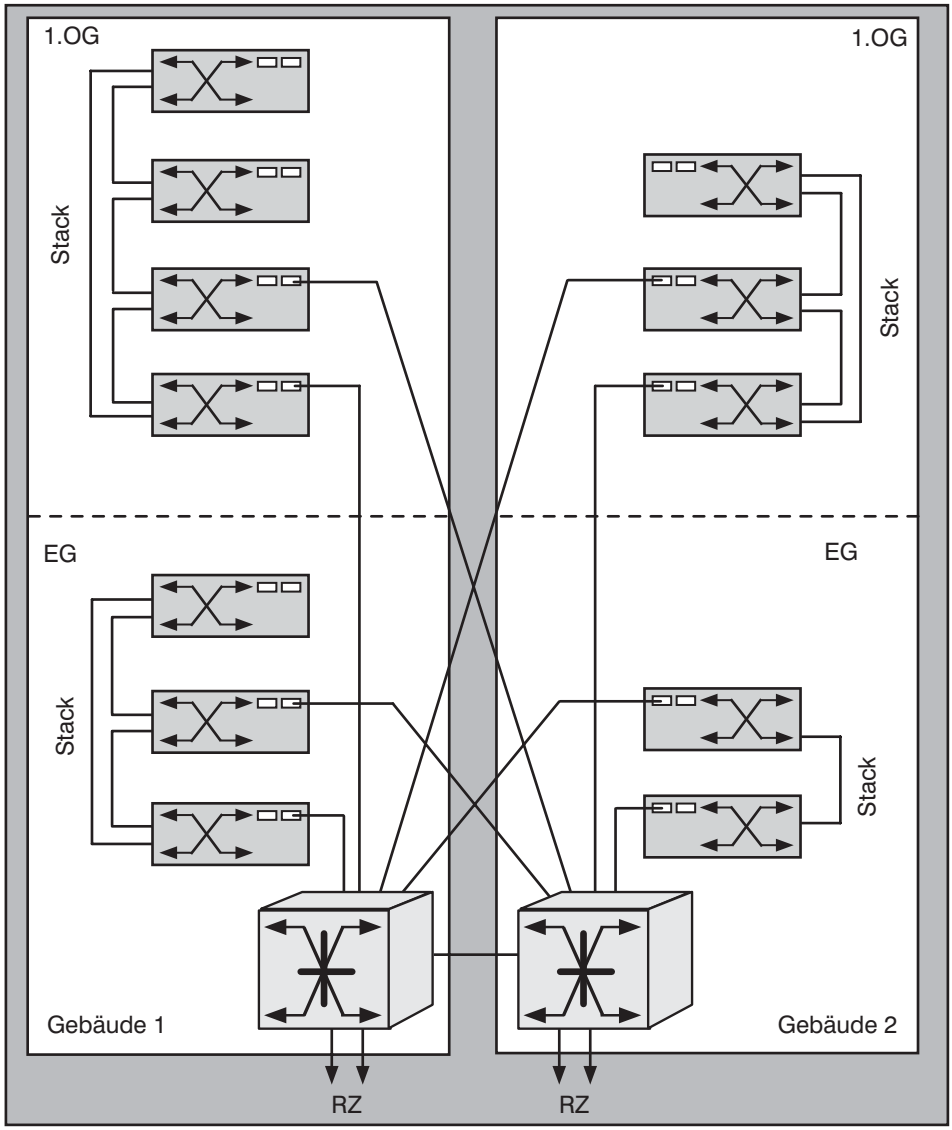


Abbildung 5.2: Redundantes Design mit Stackable Switches im Endgeräte-Bereich

24-Port Switches als PoL-Modell verfügbar, bei modularen Switches sind je Interface Karte bis zu 32 oder 48 PoL-Ports erhältlich, hier ist jedoch unbedingt auf eine angemessene Stromversorgungs-Bestückung zu achten: PoL-Module verbrauchen erheblich mehr Strom als normale Ethernet-Module. Teilweise bieten die Hersteller für unterschiedliche Modul-Bestückung unterschiedlich leistungsstarke Stromversorgungen an (bei Cisco z.B. für den Catalyst 6500 von 950 W bis zu 2500 W). Für den Alcatel OmniSwitch 7000 ist bei Einbau von PoL Modulen eine separate extern angeschaltete Stromversorgung zusätzlich zur „normalen“ Stromversorgung erforderlich.

Der Einsatz von Power Hubs bedingt zusätzlichen Platzbedarf im Verteilerschrank (ca. 2 HE je 24 bis 48 Ports) und erfordert zwei Patchungen je Anschluss: vom Datenswitch zum Power Hub, vom Power Hub zum Patchfeld. Dafür werden jedoch Abhängigkeiten zwischen Switches und Telefonen vermieden.
Insgesamt zeichnet sich aktuell aufgrund der übersichtlicheren Patchung und des geringeren Platzbedarfs ein Trend zu verstärktem Einsatz von Endspan Komponenten, d.h. PoL Switches ab. Diese werden von den Netzwerk-Herstellern auch wesentlich stärker vermarktet als Power Hubs.

5. Standortinterne-Konzepte

5.1 Netzstruktur

Für eine detaillierte Diskussion verschiedenster Layer-2 und Layer-3 Netzwerk-Konzepte verweisen wir auf den Com-Consult Research Technologie Report „Designvarianten Lokaler Netzwerke im Vergleich“. Der Betrieb von Telefonie als Echtzeit-Anwendung über IP/Ethernet Netzwerke verstärkt die Anforderung nach Redundanz, wie unter Punkt 1. und 2. dargestellt. Zur Optimierung des Betriebs im Sinne von Fehlereingrenzung, Broadcast/Multicast-Reduzierung, insbesondere auch für die TK-Server gesellen sich weitere Anforderungen hinsichtlich IP Subnetz- und VLAN-Struktur hinzu. In vielen Fällen wird ein „voice-ready“ Design IP Subnetzgrößen von 128 bis 512 Anschlüssen je Subnetz (Class C/2 bis 2fach Class C) vorsehen und für Konferenz- oder Streaming-Anwendungen die Funktionsanforderung nach Multicast-Routing mit PIM berücksichtigen. Für alle mittleren bis großen Netzwerke ist in jedem Fall die Einrichtung separater Server-Subnetze empfehlenswert. Dies gilt auch für die Einbindung von TK-Anlagen / TK-Servern. Aus den dargelegten Gründen gehen wir diesem Beitrag nur auf Design-Konzepte ein, die ab dem Etagen- / Endgeräte-Bereich vollredundant sind und Layer-3 Kopplung im Kernnetz oder mindestens zwischen Endgeräten und Servern sowie Layer-2 Kopplung im Etagen- / Endgeräte-Bereich einsetzen.

Je nach Größe der anzubindenden Gebäude oder Hallen wird ein großes Gebäude (400 bis 2000 Anschlüsse) in mehrere IP Subnetze unterteilt, ein mittleres Gebäude (150 bis 400 Anschlüsse) als ein separates Subnetz betrieben. Kleine Gebäude (20 bis 150 Anschlüsse) lassen sich gegebenenfalls bei Adressknappheit oder aus Betriebsgründen zur Vermeidung einer zu hohen Anzahl von IP Subnetzen zu einem gemeinsamen IP Subnetz zusammenfassen. Kleine Gebäude können ohne gebäudezentralen Switch betrieben und wie eine ausgelagerte Etage an den nächsten Netzsternpunkt angebunden werden.

Betrachten wir zuerst die Möglichkeiten mit Workgroup Switches, da diese die kostengünstigere Designvariante darstellen, wie unter Punkt 10. „Kosten“ näher dargelegt wird. Am liebsten vermarkten Hersteller die sternförmige, redundante Anbindung eines einzelnen Workgroup Switches an zwei gebäude- oder geländezentrale Switches. Dies führt jedoch zu einer hohen Anzahl an Uplinks und ist somit kostenintensiv (entsprechende Berechnungen sind im Report „Designvarianten Lokaler Netzwerke im Vergleich“ nachzulesen).

Workgroup Switches können fest eingebaute Gbit Ethernet Schnittstellen oder zukünftig 10 GbE Schnittstellen haben, über die sie mittels Layer-2 Kopplung kaska-

dierbar sind. In diesem Fall ist jeder Workgroup Switch STP-technisch eine separate Bridge. Erfolgt eine Anschaltung an zwei gebäude- oder geländezentrale Layer-3 Switches, so darf (soll) gemäß Standard IEEE 802.1D-2002 insgesamt eine Kaskade von maximal 7 Layer-2 Switches nicht überschritten werden, d.h. die Kaskade darf maximal 5 Workgroup Switches enthalten. Wir empfehlen hier aus Überbuchungs- und Delay-Gründen eine maximale Kaskade von vier Workgroup Switches wie in Abbildung 5.1 gezeigt. Zudem empfehlen wir für eine gute Übersichtlichkeit des Konzepts keine verteilerübergreifende Kaskadierung, obwohl dies mit passiver Durchrangierung aufgrund der vorhandenen Faserzahl vielfach möglich wäre. Sind in einem Verteilerraum weniger als 4 Workgroup Switches zu installieren, bleibt die Kaskade kleiner als 4 Switches und der Verteiler wird trotzdem redundant an das Kernnetz angeschaltet.

Stackable Workgroup Switches haben im Gegensatz zu kaskadierbaren Switches eine zusätzliche proprietäre Stackverbindung, meist auf der Rückseite (Ausnahme: Alcatel), und zusätzlich feste Uplink Ports oder ein Uplink Modul für die Anschaltung an das Kernnetz. Bei Stackable Switches ist zu unterscheiden, ob die Stackverbindung eine Kapazität von einem oder mehreren Gbit oder einem / mehreren 10 Gbit hat. Entsprechend ist die Anzahl Switchports zu dimensionieren, die in einem Stack zusammengefasst werden. Überdies ist die Anzahl stackbarer Switches herstellerabhängig und schwankt zwischen 4 bis 10 Switches je Stack. Da die Stackverbindung eine Art externe Backplane ist, zählt sie im STP nicht als Brückenverbindung, d.h. der gesamte Stack ist für die Kaskadierung wie eine einzelne Brücke zu werten. Obwohl STP-technisch die Möglichkeit gegeben wäre, empfehlen wir jedoch keine Kaskadierung mehrerer Stacks sondern die direkte Anbindung jedes Stacks an den nächsten Netzsternpunkt aus den selben Gründen wie die zuvor für Kaskaden von Workgroup Switches genannten (siehe Abbildung 5.2).

Ein Design, das in Stufe 1 vierfach Kaskaden oder Stacks verwendet, ist in weiteren Ausbaustufen auf zweifach Kaskaden oder Stacks erweiterbar bis hin zur Einzelanbindung von Switches, soweit eine zukünftige Laststeigerung dies erfordert. Eine Erweiterung von vierfach Kaskaden / Stacks auf zweifach Kaskaden / Stacks ist in Abbildung 5.3 gezeigt. Hier wird deutlich, dass die Erweiterung die doppelte Anzahl Interfaces in den zentralen Layer-3 Switches kostet.

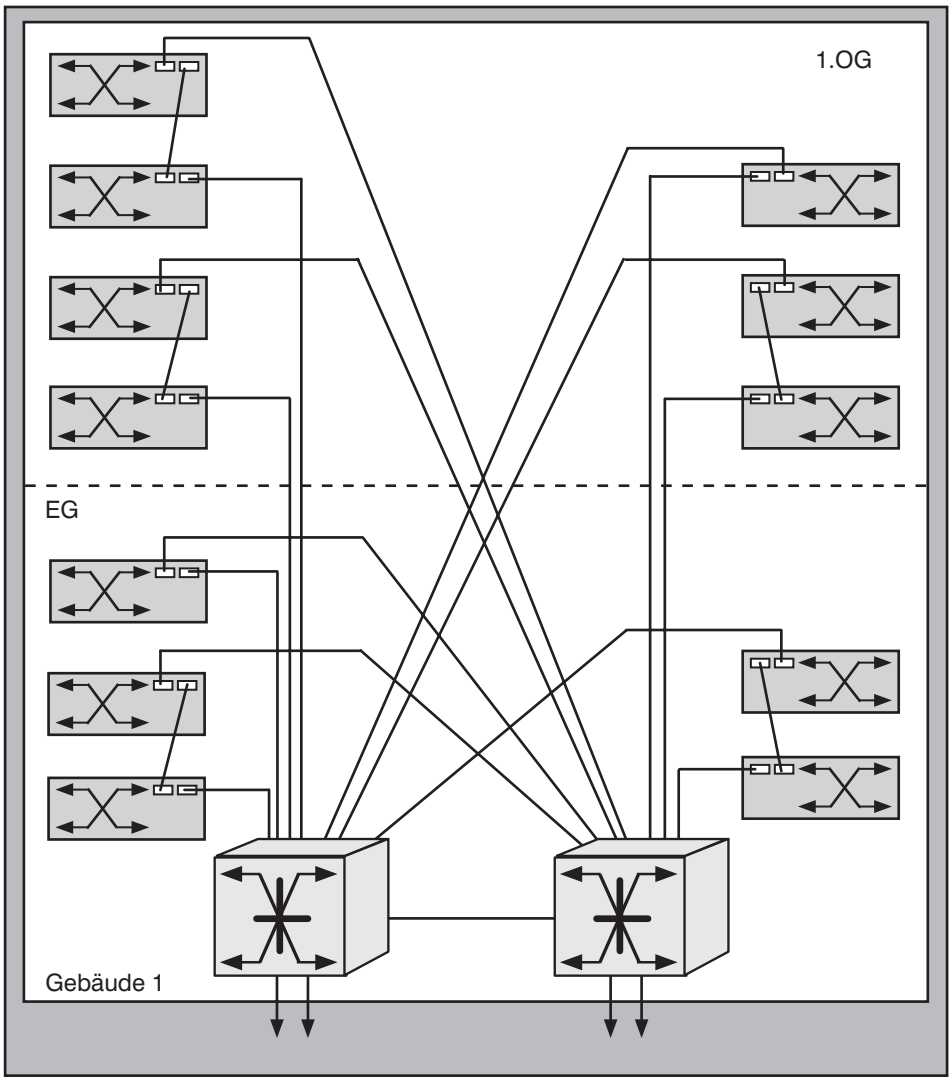


Abbildung 5.3: Redundantes Design mit zweifach kaskadierten Switches im Endgeräte-Bereich

Alternativ zu Workgroup Switches können in den Etagenverteilern auch modulare Switches eingesetzt werden, im Regelfall ein Switch je Etagenverteiler (siehe Abbildung 5.4). Bei geringer Anzahl von Anschlussports (< 50) ist dies mit sehr hohen Pro-Port-Kosten verbunden, daher kommt das Konzept in Hallenbereichen mit geringer Anschlussdichte kaum zum Einsatz. Bei höherer Anschlussdichte muss der Switch zur Minimierung der von SPoF Problematik mindestens mit redundanter Stromversorgung, möglicherweise auch mit redundanter CPU bestückt werden. Vorteile modularer Switches liegen in einer höheren Systemleistung und einer höheren Summenleistung für Uplink-Verbindungen, da hier mehrere Gbit-Schnittstellen mit Link Aggregierung gebündelt werden können, was bei Stacklösungen nur selten über mehrere gestackte Switches hinweg möglich ist. Eine zukünftige Hochrüstung auf mehrere 10 Gbit Module ist nur bei modularen Switches als Erweiterung möglich, da für Workgroup Switches aktuell noch keine flexibel nachrüstbaren 10 Gbit Erweiterungsmodule zur Verfügung stehen. Auch zur Reduzierung der Komponentenvielfalt (von 2 Komponenten auf 1 Komponente) und Vereinheitlichung von Konfiguration und Management wird dieses Konzept teilweise gewünscht, wir verweisen jedoch hierzu auf die Kostenbetrachtung unter Punkt 10.

Falls eine LWL-Verkabelung bis zum Endgeräteanschluss (z.B. aus Platzmangel, vielfach in denkmalgeschützten Gebäuden) verlegt wurde, sind jedoch vielfach nur noch modulare Switches einsetzbar, da die Workgroup Switches mit 100 Mbit LWL-Ports End of Life gehen und kostengünstige Workgroup Switches mit Gbit LWL-Ports bzw. GBIC‘s nicht vermarktet werden. In diesem Fall gibt es mit IP Telefonen jedoch ein grundsätzliches Problem: Es gibt keine Telefone mit LWL

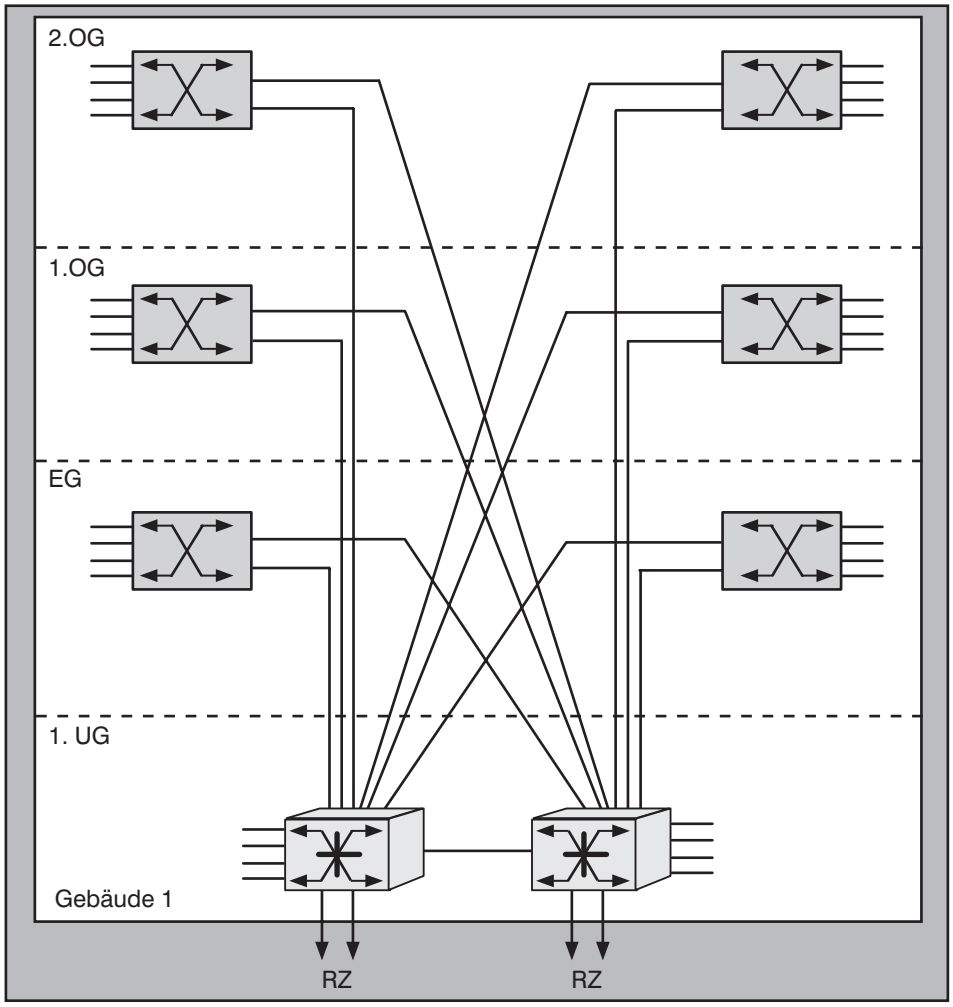


Abbildung 5.4: Redundantes Design mit modularen Switches im Endgeräte-Verteiler

Ethernet-Anschluss! Soll bei LWL-Verkabelung bis zum Endgerät IP Telefonie eingesetzt werden, so muss zur Anschaltung der Telefone auf LWL-Kupfer-Konverter zurückgegriffen werden.

Migration zu 10 GbE im Backbone und 1 Gbit am Endgerät

Die aktuell verfügbaren Netzkomponenten unterstützen anfänglich 10 Gbit Ethernet, mit einzelnen Ports bei Workgroup Switches und 1-Port bis maximal 6-Port Karten bei modularen Switches. Allerdings sind keine Telefone mit Gbit Ethernet Anschluss verfügbar, hier ist entsprechend Autonegotiation (soweit sie problemlos funktioniert) oder Festkonfiguration der Switchports auf 100 Mbit zu konfigurieren. Ebenso wird die Anbindung von TK-Servern über 10 Gbit Ethernet aktuell nicht unterstützt.

5.2 Standort von TK-Servern und Gateways

In dem Maße, wie sich die klassische TK-Anlage zum TK-Server wandelt, spätestens wenn als zentrale Steuerkomponente ein Standardserver mit Windows, Linux oder Unix als Softswitch eingesetzt wird, ist der Standort dieses TK-Servers das RZ beziehungsweise der Serverpool. Ob für TK-Server ein eigener Server-Pool aufgemacht wird oder diese im allgemeinen RZ / Serverpool der IT betrieben werden, hängt sicher auch von der organisatorischen Eingliederung der TK-Be-

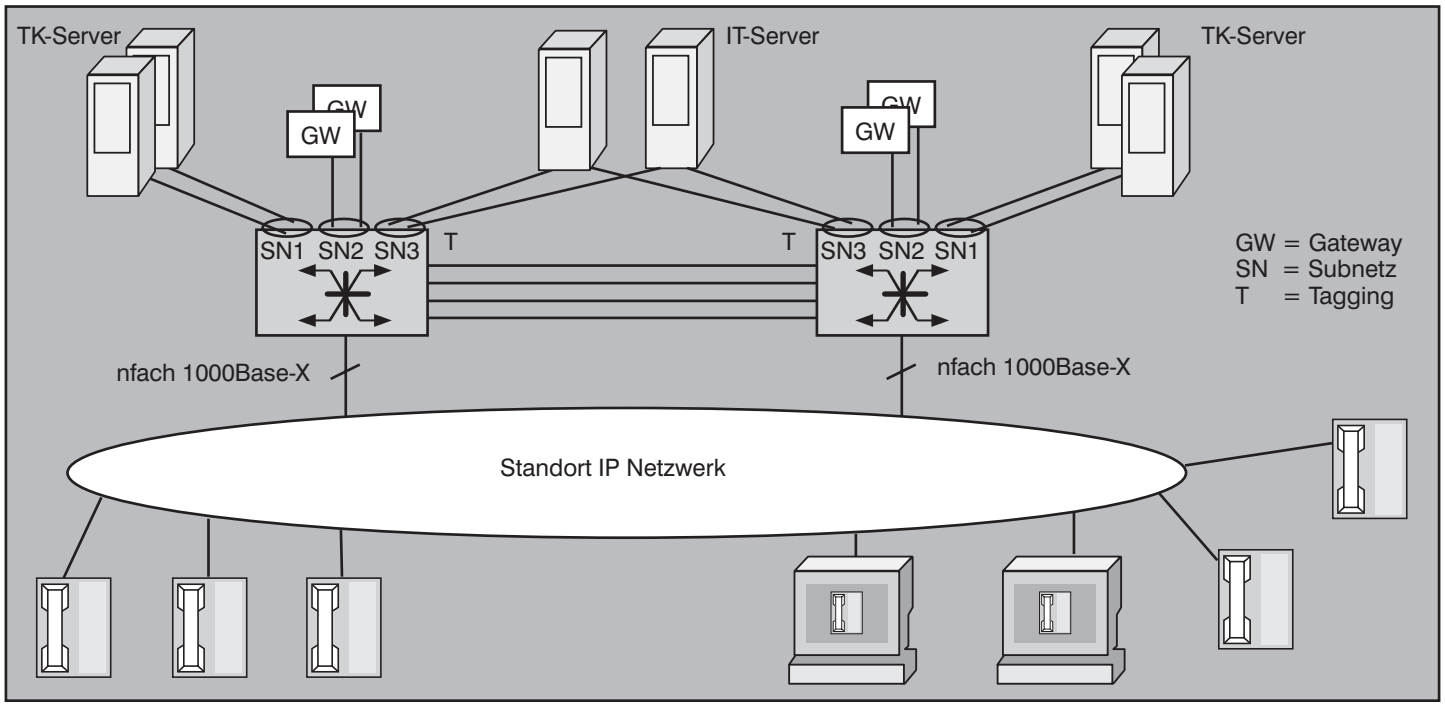


Abbildung 5.5: Positionierung von TK-Servern im RZ mit Konfiguration separater IP Subnetze

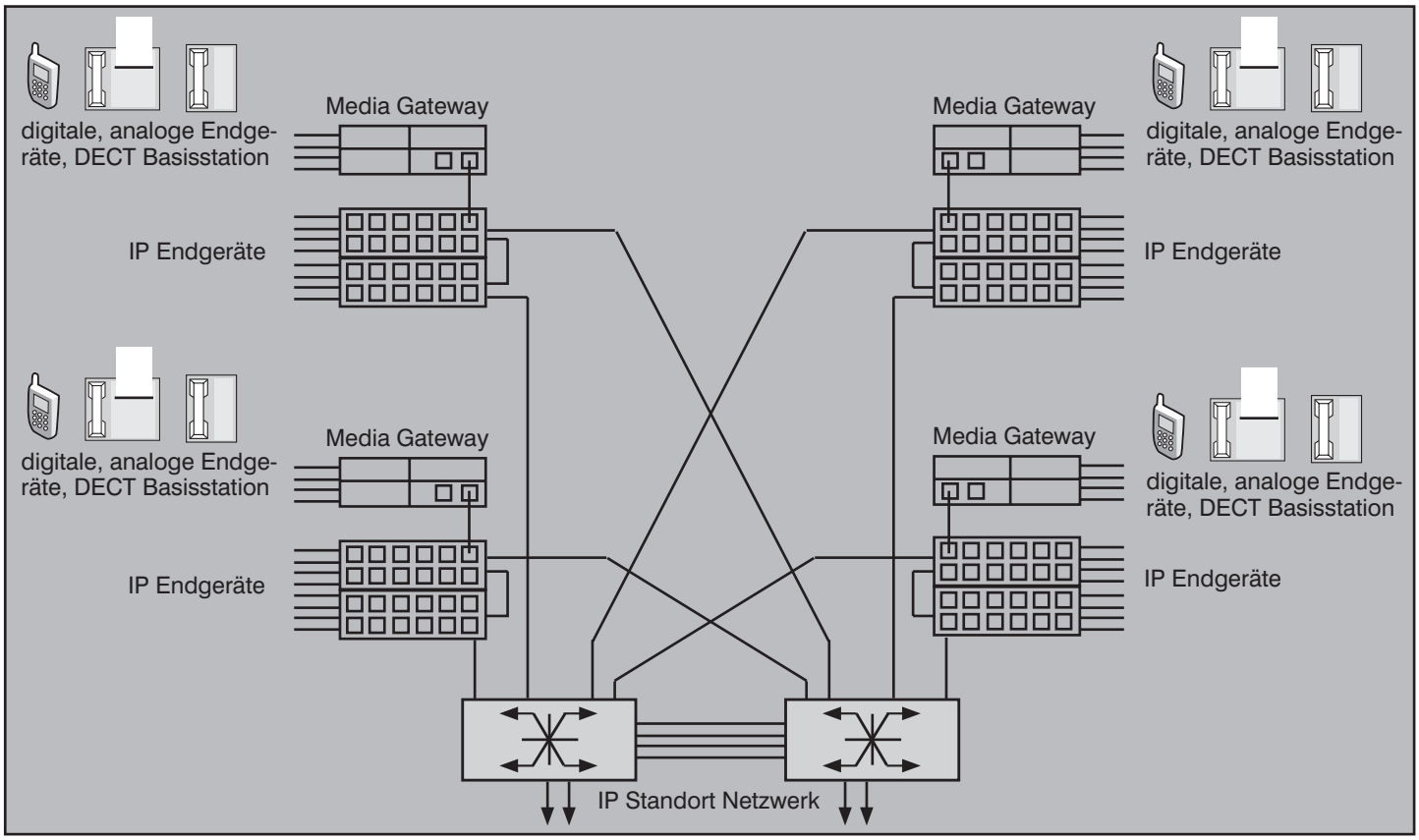


Abbildung 5.6: Dezentrale Positionierung von Media Gateways

triebsgruppe ab. Je höher die Backup-Anforderungen sind, desto eher wird der TK-Backup-Server in einem zweiten Serverraum bis hin zu einem weiter entfernten Katastrophen-Rechenzentrum positioniert werden, mit entsprechend hoher Bandbreite zur Verbindung von Produktivnetz und Katastrophen-RZ, insbesondere bei lastverteilter Nutzung von Default und Backup-Servern.

Wird ein IP-fähiges Chassis-System eingesetzt, müssen viele klassische Anschlüsse eingebunden werden und laufen diese in einem bereits vorhandenen separaten TK-Raum auf, so wird dieses Chassis-System wohl ebenso wie die zuvor genutzte TK-Anlage in genau diesem Raum betrieben werden.

Um TK-Server gegen Störfälle im IT-Serverpool abzuschirmen, besonders bei proprietären Clusterlösungen mit Layer-2 Kopplung, können für die TK-Server ein oder mehrere separate IP Subnetze eingerichtet werden. Mittels entsprechender Portgruppen-Definition auf den im Serverpool betriebenen Layer-3 Switches ist dies leicht konfigurierbar. Für einen noch weiter reichenden Schutz können TK-Server in einer eigenen DMZ betrieben werden und überhaupt nicht mittels Routing mit dem IT-Serverpool gekoppelt sein. Hier entsteht jedoch die Schwierigkeit, multifunktionale Endgeräte (z.B. PC‘s) mittels Layer-3 Kopplung an den TK-Server anzuschalten, den gesamten TK-Betrieb jedoch per Firewall-Kopplung vom IT-Betrieb zu isolieren. Im Regelfall ist dies nur für Hardware-Telefone vernünftig umsetzbar, die keine IT-Anwendungen (Web, CTI ...) nutzen. Es gibt auch Hersteller, die die Einrichtung separater und völlig isolierter

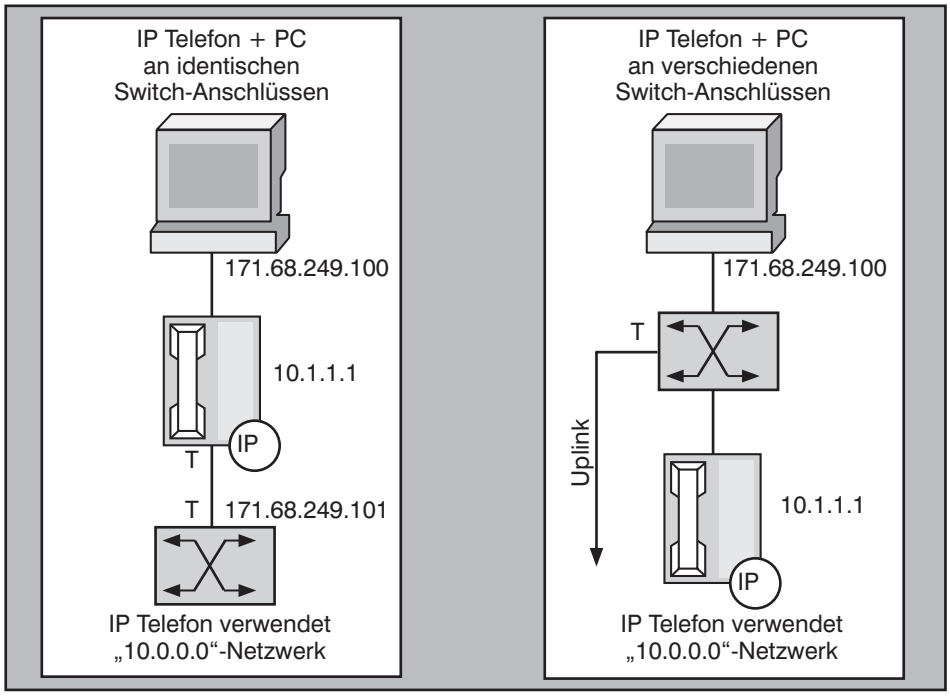


Abbildung 5.7: Einsatz separater VLAN‘s / IP Netze für Telefone

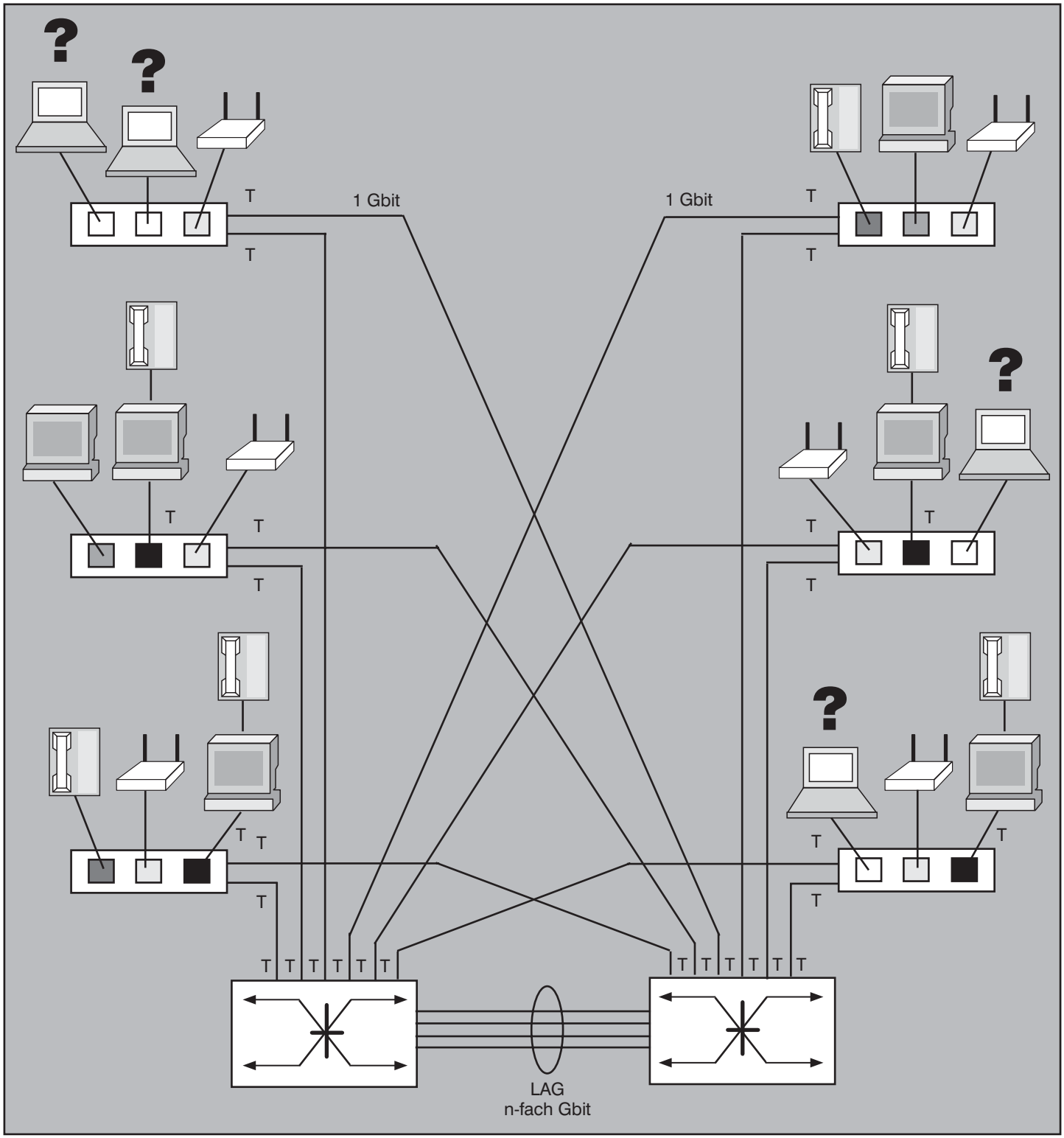


Abbildung 5.8: VLAN-Separierung für verschiedene Benutzergruppen wie Telefone, WLAN, Laptops

Management-Netze für TK-Server empfehlen (z.B. Avaya) und diese mit einem isolierten Outband Ethernet Management Port ausstatten.
TK-Server, die Benutzer bedienen, welche über externe Einwahl (RAS, VPN oder ähnliches) auf den Server zugreifen, sollten in einer separate DMZ betrieben werden, um das Risiko zu minimieren, dass bei Kompromittierung eines extern erreichbaren IT-Servers im zweiten Schritt der TK-Server kompromittiert werden kann.

Für Zusatz-Server mit TK-Applikationen (UM, CTI, CC) und Gateways gelten die gleichen Aussagen wie für TK-Server: Aus Sicherheitsgründen und zur Erhöhung der Verfügbarkeit können TK-Zusatzserver und insbesondere PSTN-Gateways in separaten IP Subnetzen betrieben werden. Mindestens ist jedoch eine Layer-

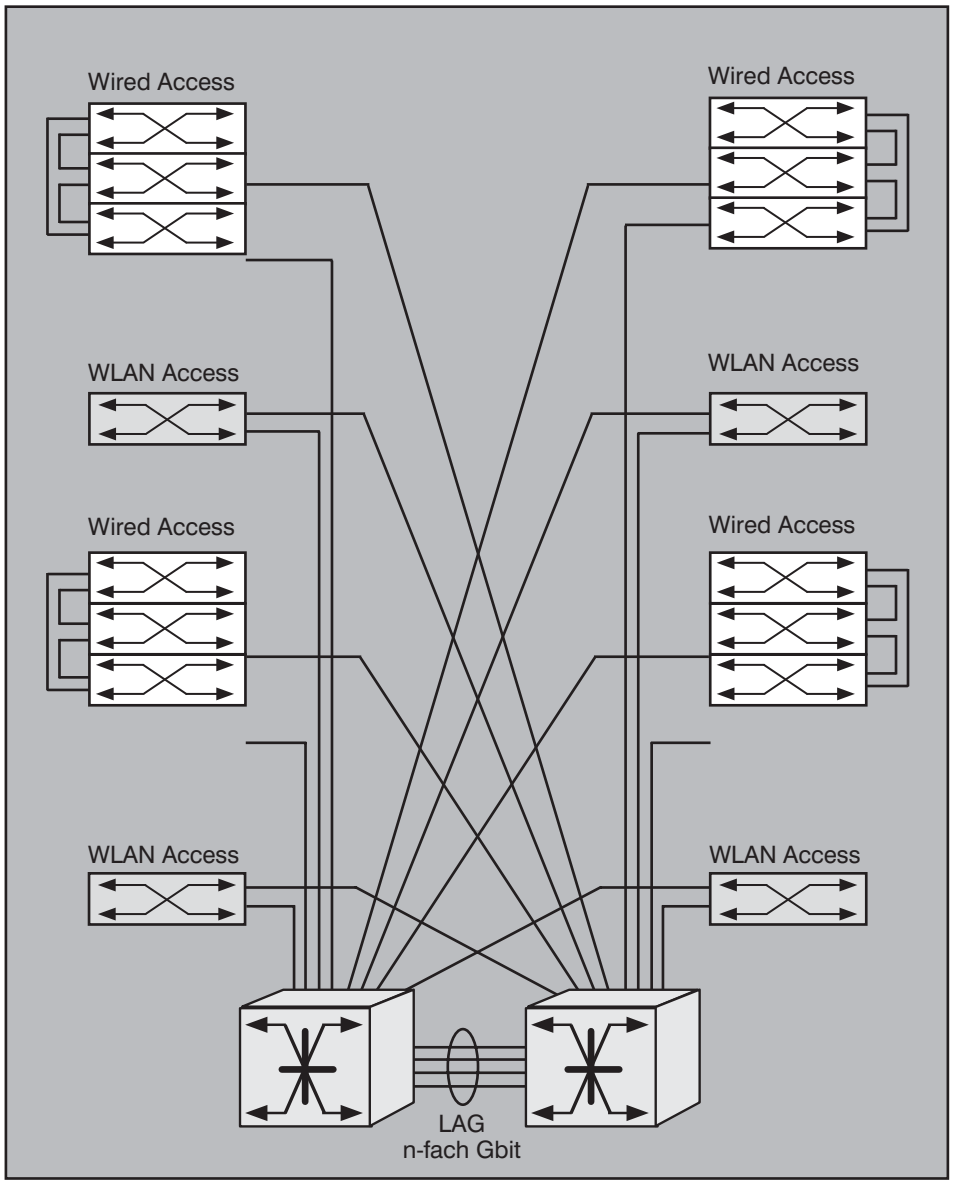


Abbildung 5.9: VLAN-Separierung für versch. Benutzergruppen wie Telefone, WLAN, Laptops

2 Kopplung zwischen Endsystemen und Gateways bzw. TK-Applikationsservern zu vermeiden. Eine Übersichts-Grafik zeigt Abbildung 5.5.

Werden nicht nur PSTN-Gateways sondern bei dezentralen Hybrid-Konzepten auch Media Gateways zur Integration analoger, digitaler oder DECT Anschlüsse eingesetzt, so ist die Verteilung auf dezentrale Standorte zu berücksichtigen, z.B. Verteilung auf die Gebäude bzw. Unterverteiler, in denen diese Anschlüsse bei vorhandener sternförmiger TK-Verkabelung auflaufen. Durch den dezentralen Einsatz von Media Gateways oder Access Points (wie unter Punkt 3. beschrieben), lässt sich die Anzahl der von einem Single Point of Failure betroffenen Anschlüsse weiter reduzieren. Eine Übersichtsgrafik zeigt Abbildung 5.6.

5.3 Trennung von Benutzergruppen

Häufig genannte Argumente oder Anforderungen, um spezielle Benutzergruppen vom allgemeinen Netzwerk abzusondern, sind

- Verfügbarkeit
- Leistung (Durchsatz, Antwortzeit)
- Sicherheit

Beispiele für solche Benutzergruppen sind

- SPS‘en, Produktionsnetze (Verfügbarkeit, Antwortzeit)
- Objektschutz (Verfügbarkeit)
- Telefone (Durchsatz, Antwortzeit, Sicherheit)
- Wireless Benutzer (Sicherheit)
- Management (Verfügbarkeit, Sicherheit)
- Monitoring (Verfügbarkeit, Sicherheit)

Port-basierte VLANs

Ein oft vermarkteter Ansatz zur Umsetzung solcher Anforderungen für Telefonie ist die Definition separater Telefonie-VLAN‘s, die dann mit unterschiedlicher Funktionalität an das Datennetz gekoppelt sind, im einfachsten Fall mittels Routing / Layer-3 Switching, im komplexeren Fall mittels Firewall-Verbindung, im Extremfall völlig isoliert. Der letztgenannte Fall bedeutet, dass keine integrierte Daten- / TK-Anwendungen möglich sind, die auf „normale“ IT-Server wie Verzeichnisse, DNS-Dienst, DHCP-Dienst, Datenbanken etc. zugreifen. Als Konsequenz ergibt sich eine entsprechend reduzierte TK-Funktionalität ohne Zusatzanwendungen wie z.B. CTI und Kollaboration. Dafür ist die erreichbare Sicherheits-Abschottung relativ hoch. Eine weitere Hoffnung ist, mit separaten Telefonie-VLAN‘s einen einfachen Ansatz für implizite Priorisierung des Telefonie-Verkehrs gefunden zu haben (Policy: Bearbeite alle Pakete mit dem VLAN Tag 122 mit der Priorität „Hoch“).

Die genannten VLAN‘s lassen sich über feste Portzuordnung konfigurieren, indem alle Switchports, an denen Telefone angebunden sind, einem entsprechenden VLAN zugeordnet und alle weiter kaskadierten Uplinks als getagte Verbindungen konfiguriert werden. Wird die kaskadierte Lösung PC – Telefon eingesetzt, so muss ab dem Miniswitch im Telefon bis zum nächsten Layer-3 Switch Tagging (T) konfiguriert werden. Kaskadierte und nichtkaskadierte Anschaltung mit Konfiguration separater VLAN‘s ist in Abbildung 5.7 dargestellt. Im Normalfall wird jedes VLAN einem eigenen IP Subnetz zugeordnet, so dass die Einrichtung separater Telefon-VLAN‘s gleichzeitig die Einrichtung von separaten IP-Subnetzen für Telefonie bedeutet. Zusätzlich sind an dieser Stelle einige Fragen zu klären, deren Antwort jeweils projektspezifisch gefunden werden muss (siehe hierzu Abbildung 5.8):

- Welchem VLAN / IP Subnetz werden Ethernet PC‘s und Laptops mit Softphone zugeordnet?
- Welchem VLAN werden WLAN Telefone zugeordnet?
- Welchem VLAN werden WLAN Laptops mit Softphone zugeordnet?
- Welchem VLAN werden (zukünftig) Bildschirmtelefone mit Webzugang zugeordnet?

Eine denkbare, noch einigermaßen übersichtliche Lösung für das in Abbildung 5.8 gezeigte Szenario ist das Vorhalten fes-

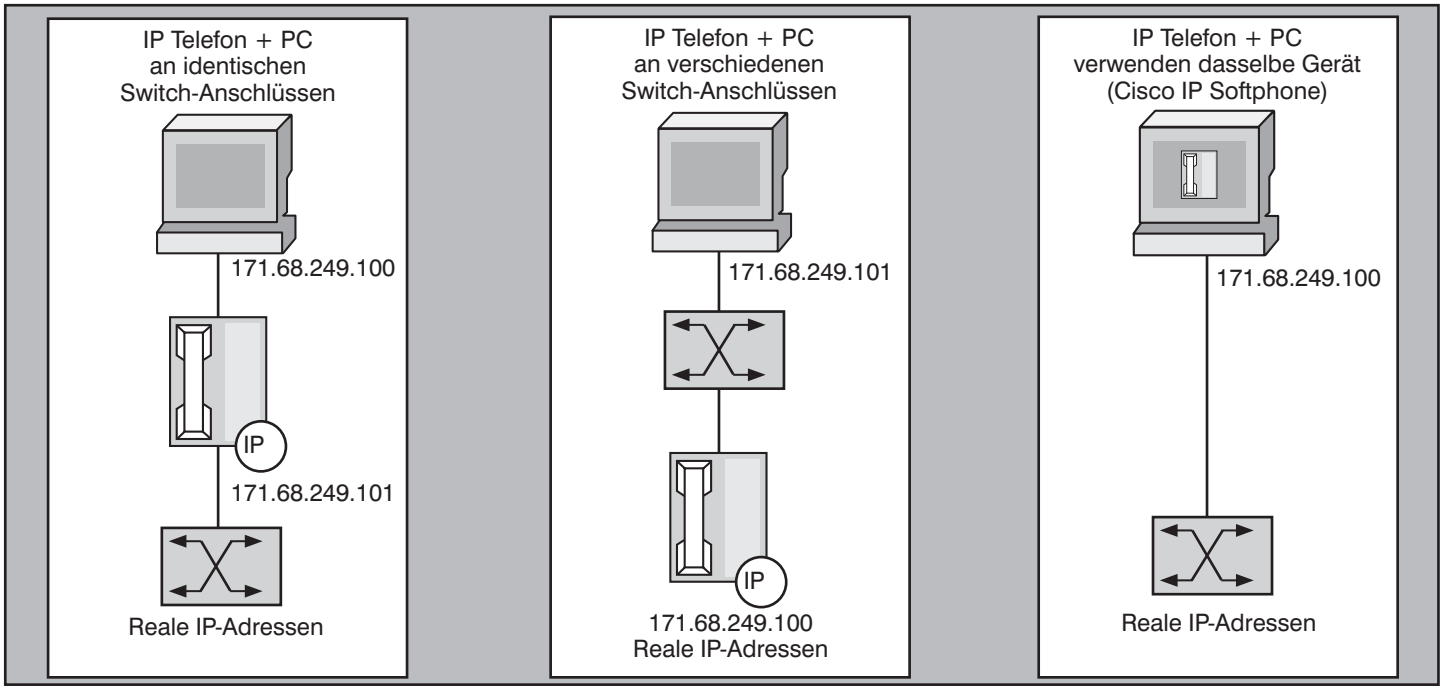


Abbildung 5.10: Einsatz gleicher VLAN‘s / IP Netze für Telefone und PC‘s

ter Ports je Etagenswitch für Wireless und Monitoring, die Zuordnung von WLAN Telefonen zum Wireless VLAN, die Zuordnung von IP Handapparaten zu separaten Telefonie-VLAN‘s und die Zuordnung aller Softphones zu den jeweiligen allgemeinen Etagen-Subnetzen (sowohl bei Wireless als auch bei Wired Laptops / PC‘s). Allerdings wird schon aus der Grafik ersichtlich, dass diese Lösung zu einer deutlichen VLAN-Zersplitterung und erzwungenem Tagging für alle Uplinks führt. Zudem schafft diese Zuordnung für Telefonie eine Zwei-Klassen-Gesellschaft, in der Softphones anders behandelt werden als Hardphones, da sie den jeweiligen „Daten-Subnetzen“ zugeordnet werden. Der pragmatische aber generische Ansatz ist hier, auf eine VLAN-Zuordnung zu verzichten und Telefone, PC‘s mit Softphone, und PC‘s ohne Softphone gleichermaßen dem jeweils für diesen Etagenbereich vorgesehenen IP Subnetz zuzuordnen, wie in Abbildung 5.10 gezeigt. Eine Reduzierung der VLAN Zersplitterung ist bei flächendeckender WLAN Ausstattung möglich (siehe Abbildung 5.9), wenn für die Ethernet-Anschaltung der WLAN Access Points in jedem Verteiler ein separater Ethernet Switch vorgehalten wird (Kostenfaktor: hier wird Übersichtlichkeit mit Mehrinvestition bezahlt).

Automatische VLAN-Zuordnung

Als Alternative für die Zuweisung von VLAN‘s durch feste Portzuordnung können einige IP Telefonie-Lösungen eine automatische VLAN-Zuordnung für Telefone vornehmen, sobald der Switch an der MAC-Adresse (Hersteller OUI!) erkennt, dass das angebundene Endgerät ein Telefon ist. Gleiches gilt für eine automatische VLAN-Zuordnung in Kombination mit Authentifizierung nach dem IEEE Standard 802.1X (Port Security). Beide Alternativen führen jedoch wiederum zu der schon zuvor genannten Zwei-Klassen-Gesellschaft für Hardphones und Softphones und stellen somit keine generische Lösung zur Verfügung.

Soll eine Priorisierung von IP Telefonie erreicht werden, so ist die einzige gene-

rische, d.h. auf alle Handapparate und Softphones anwendbare Lösung das Setzen von Priorisierungs-Bits im IP und MAC Header durch die Anwendung bzw. das Endgerät selbst. Aber auch diese Lösung hat einen Haken: In den beteiligten Switches muss explizite Priorisierung aktiviert werden, d.h. Lesen des Headers, Auswertung etwa gesetzter Priorisierungs-Bits und entsprechend hochpriorige oder niederpriorige Bearbeitung des Paketes. Dies öffnet jedoch kreativen Benutzern ein Scheunentor, die beliebige andere Anwendungen (mit Tools, die aus dem Internet herunterladbar sind) ebenfalls so konfigurieren, dass die Priorisierungs-Bits auf einen hohen Wert gesetzt werden. Hier gibt es keine technische Lösung, da selbst die ausgefeiltesten Policy- und Filter-Regeln abgesehen vom immensen Betriebsaufwand nicht alle Anwendungen einfangen werden. Übrig bleibt nur den Pragmatiker-Ansatz: Hinzunehmen, dass einige wenige kreative Benutzer die Regeln brechen. Erfahrungsgemäß ist die Anzahl dieser Benutzer in vielen Unternehmen niedrig.

6. Abkürzungen

API	Application Programming Interface
AV	Audio / Video
Codec	Codierer / Decodierer
CPU	Central Processing Unit
CTI	Computer Telefonie Integration
DECT	Digital Enhanced Cordless Telecommunication
DPNSS	Digital Private Network Signalling System
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
ECMP	Equal Cost Multipath
GK	Gatekeeper
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
GW	Gateway
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Protection System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informations-Technologie
ITSP	Internet Telephony Service Provider
JPEG	Joint Photographic Experts Group
JSAPI	Java Speech API
JTAPI	Java TAPI
LAG	Link Aggregation Group
LAN	Local Area Network
LSP	Local Survivability Processor
MAC	Media Access Control
MCDN	Meridian Customer Defined Network (Nortel)
MPEG	Motion Pictures Expert Group
MST	Multiple Spanning Tree
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NIC	Network Interface Card
OSPF	Open Shortest Path First
PDA	Personal Digital Assistant
PIM	Protocol Independent Multicast Routing
PoE	Power over Ethernet
PoL	Power over LAN
PSTN	Public Switched Telephony Network
PSU	Power Supply Unit
QSIG	Q-interface SIGnalling protocol
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RIP	Routing Information Protocol
RTC	Real-Time Communication
RTP	Real-time Protocol
RST	Rapid Spanning Tree
RSTP	Rapid Spanning Tree Protocol
RZ	Rechenzentrum
SIP	Session Initiation Protocol
SPoF	Single Point of Failure
SRST	Survivable Remote Site Telephony
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TAPI	Telephone API
TCP	Transmission Control Protocol
TK	Telekommunikation
TP	Twisted Pair
UDP	User Datagram Protocol
UM	Unified Messaging
USB	Universal System Bus
USV	Unterbrechungsfreie Stromversorgung
VLAN	Virtual LAN
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPN	Virtual private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WLAN	Wireless LAN
XML	eXtended Markup Language

Fortsetzung folgt!

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
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
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